ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ

ІІ Міжнародна науково-технічна конференція

Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку

КИЇВ - 2022

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ
ІМЕНІ ГЕРОЇВ КРУТ

ІІ МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

“Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку”

1 грудня 2022 року

(Доповіді та тези доповідей)

Київ – 2022

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів II Міжнародної науково-технічної конференції “Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку” опубліковано доповіді та тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад’юнктів, здобувачів, курсантів Військового інституту телекомунікацій та інформатизації імені Герої Крут та інших вищих навчальних закладів, представників промисловості в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення, застосування підрозділів, комплексів, засобів зв’язку та автоматизації в операції Об’єднаних сил. Метою конференції є аналіз стану та обмін досвідом з питань систем і технологій зв’язку, інформатизації та кібербезпеки з урахуванням досвіду застосування у Збройних Силах України.

ЗМІСТ

Доповіді

Тези

DrS Vyacheslav Kharchenko (NAU KhAI)

AUTONOMOUS MOBILE SYSTEMS, INTERNET OF SMART THINGS, ARTIFICIAL INTELLIGENCE: SYNERGY FOR CYBERSECURITY AND SAFETY

1. Background

The reportoverviews problems and solutions of utilizing Artificial Intelligence (AI), Internet of Things, especially Smart Things (IoST), to ensure the safety and cybersecurity of autonomous transport systems (ATSs)in different domains such as aviation, space, and maritime as well as objects of critical infrastructures, first of all, NPP I&Cs and smart grids. The results presented are based on the several on-going projects that are developed by Department of Computer Systems. Networks and Cybersecurity, National Aerospace University KhAI, in particular:

- R&D Project ECHO "European Network of Cybersecurity Centres and Competence Hub for Innovation & Operations", 2019-2023 (funded by EU Program Horizon 2020);
- R&D&I Project AvioCore 4.0 "German-Ukrainian Core of Excellence in Digitization Research in Domains Industry 4.0 (KhAI,Kharkiv), 2021-2024(funded by German Government);
- R&E Project CyberEDU "MSc and PhD Studies and Research Activities in Cybersecurity of Industrial Control Systems" (funded by Swedish Institute, Stockholm);
- National R&D projectsdedicated to development and research:
• Dependable UAV Fleets for Intelligent Monitoring Systems of Critical Objects (2021-2023),
• Methods and technologies for Dependable Industrial IoT (2022-2023),
• Safety and Cybersecurity of SMR Digital Infrastructure (2022-2024)
(funded by Ministry of Education and Science of Ukraine) and others.

2. Approach

Approach to research is grounded on concepts of Big Safety joining functional safety, information and cybersecurity, physical IT-security and other attributes [1].

Strategy of research and development is based on:

-search of synergy that can be got due to application of modern information and mobile technologies critical domains to assure safety and security, and

- minimization of risks of safety and security deficits caused by new threats, vulnerabilities, cyber attacks and unspecified failures related to such technologies as AI, IoT, Cloud and Edge computing, Augmented and Virtual Reality and so on.

An example of such approach is illustrated by application of Internet of Things. On the one side, IoT and IoST increase possibilities and allow implementing new generation of systems for monitoring of critical objects and assurance of their safety and security. However, application of IoT is accompanied by increasing of nodes and communications, transmitted data capacity and, hence, increasing of threats, vulnerabilities, potential attacks and failures which can cause emergencies. The following expressions, that are not strong mathematical formulas, describe these circumstances [2]:

IoT = IoT (Internet of Things = Internet of Threats),

IoE = IoE (Internet of Everything = Internet of Emergencies).

Hence, Von Neumann paradigm "reliable systems out of unreliable components" can be formulated for IoT application by following way: safe/secure IoT based systems out of unsafe (or not enough safe)/ insecure (or not enough secure) nodes and communications. To implement this paradigm interaction of physical and information environment and IoT system should be considered in detail according with general model [3]. Other example of the approach implementationisillustrated by research dedicated to application of AI to assure cybersecurity and safety of autonomous transport systems [4]. There are the following directions for investigation and development:

a) AI for cybersecurity assurance of ATSs including: prediction (threats, vulnerabilities, attacks); prevention (analysis and initializationof countermeasures); detection (attacks and effects assessment); tolerance (choice and implementation of mitigation procedures); recovery (choice and initialization of

assets recovery); relearning (analysis of cases, identifying means and ways of relearning, accumulating experience, and enhancing proactive decision-making algorithms);

b)set of AI algorithms, models, software/hardware platforms (AIware) as an object of attacks: AIware components;threats, vulnerabilities, and attacks on different levels of AIware components; metrics of criticality; set of countermeasures;AI-based penetration testing;

c) AI for generation of so-called artificial intelligence-powered attacks: objects and goals of white/ethical hacking; kinds of attacks generated by AI support;means for implementation of AI-powered attacks;metrics of efficiency;

d) AI-based protection against AI-powered attacks. In fact, this case of AI application is a part of the goal "a" in recognition of specific features of AI-powered attacks.

3. R&D directions

The following research and development joining AI, IoSTand mobile technologies in context of safety and cybersecurity are analysed:

- AI and AI platforms: models of quality, metric based assessment, tools;
- ethics and human-centric AI characteristics profiling and assessment;
- (explainable) XAI as a Service: quality models, cybersecurity and experiments;
- application of AI for ATSs resilience consideringsecurity informed safety approach;
- evolutionanalysis of software quality models considering AI development and implementation;
- IMECA and penetration testingbased analysis of cybersecurity and safety for robotic systems;
- AI and Internet of Drones based UAV fleets for monitoring/identification of unsafe objects and territories(including demining tasks);
- combining of Markov's and semi-Markov's chains, risk matrix and Bayesian analysis for assessment of safety and securitycritical systems (energy grids, cloud services, IoT systems).

KEY PUBLICATIONS

1. Kharchenko, V., Yastrebenetsky, M. About Concept of Big Safety //*Reliability: Theory and Applications*, 2021, 16(1).

2. Kharchenko, V. Big Data and Internet of Things for Safety Critical Applications: Challenges, Methodology, Industrial Cases //*Intern. Journal on Inform. Technologies and Security*, 2018, No. 4.

3. Kharchenko, V: Independent Verification and Diversity. The Echelons for Assurance of Cyber Physical Systems Safety.ICTES WS Proceedings 2762, CEUR-WS.org 2020.

4. Kharchenko, V., Illiashenko, O., Fesenko, H., Babeshko, I. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis // Seria "*Communications in Computer and Information Science*", 2022, vol 1689. Springer, Cham.

5. Kharchenko, V., Fesenko, H., Illiashenko, O. Basic model of non-functional characteristics for assessment of artificial intelligence quality. *Radioelectronic and Computer Systems,*2022,2(102).

6. Kharchenko, V.,Fesenko, H.,Illiashenko, O. Quality Models for Artificial Intelligence Systems: Characteristic-Based Approach, Development and Application //*Sensors*, 2022, 22, 4865.

7. Lysenko, S.Bobrovnikova, K., Kharchenko, V., Savenko, O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency //*Algorithms*, 2022, 15(7),239.

8. Kharchenko, V.,Kliushnikov, I., Rucinski et.al. O. UAV Fleet as a Dependable Service for Smart Cities: Model-Based Assessment and Application //*Smart Cities* 2022, 5

9. Kharchenko, V.,Ponochovnyi, Y., Ivanchenkoet. al. Combining Markov and Semi-Markov Modelling for Assessing Cybersecurity of Cloud and IoT Systems //*Cryptography,2022, 6,* 44.

10. Kharchenko, *V.,* Illiashenko, O., Sklyar, V. Invariant-Based Safety Assessment of FPGA Projects: Conception and Technique // *Computers,* 2021, 10, 10.

11. Torianyk, V., Kharchenko, V.,Zemlianko, H. IMECA Based Assessment of Internet of Drones Cyber Security Considering RF Vulnerabilities.Proceedings of IntelITSIS 2021: 460-470.

12. Babeshko, I., Illiashenko, O., Kharchenko, V.,Leontiev, K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques //*Mathematics* 2022, 10, 2297.

doctor in technical science Lyudmila Kovalchuk (Igor Sikorsky Kyiv Polytechnic Institute)
Roman Oliynykov (V.N. Karazin Kharkiv National University)

A GRINDING ATTACK ON SLOT LEADERS ELECTION PROCEDURE FOR POS-BASED BLOCKCHAINS WITH ON-CHAIN RANDOMNESS GENERATION

1. Introduction

Tezos is a decentralized cryptocurrency based on a pure Proof-of-Stake (PoS) consensus protocol [1-3]. There are two types of participants in Tezos: bakers who create blocks and endorsers who agree on blocks. To become a baker or endorser, it is needed to have at least 8000 coins (a minimum stake which is called a roll). If a user does not have enough coins to participate in the protocol, he can use delegation.

Blocks in Tezos are grouped into cycles. The lists of bakers and endorsers are determined at the beginning of a cycle by a follow-the-satoshi strategy starting from a random seed computed from information already found on the blockchain.

A grinding attack [4] affects PoS systems by exploiting the lack of randomness in the block producer election procedure. In this case, a participant can manipulate election process and increase his chance to be elected as a block producer.

Our results. In this paper we formulate simple and generalised versions of grinding attack on the procedure of bakers election in Tezos protocol. We obtained formulas for probabilities of both versions of this attack and calculated corresponding numerical results for different stake ratio of adversary. The results obtained show that to get a half or more blocks in a whole cycle, the adversary need to have stake ratio not less than $p = 0.44$ to implement simple version of attack and not less than $p = 0.4$ to implement its generalised version.

2. Description of bakers election and grinding attack

In this section we give description of the procedure of bakers election [2] and informal description of the grinding attack on this procedure. The formal description of the attack will be given in the next section.

As it was mentioned, the whole process of block generation in Tezos is divided into cycles. Each cycle with the number i is associated with a random seed which is used for a random selection of a roll snapshot from cycle with the number $i-2$ and the rolls in this snapshot. The selected rolls determine the baking and endorsing rights in the cycle i +PRESERVED_CYCLES (in the mainnet PRESERVED_CYCLES = 5 cycles; a branch whose fork point is in a cycle more than PRESERVED_CYCLES in the past is not accepted).

The random seed for the cycle with the number i is a 256-bit number generated at the very end of the cycle with the number $i-1$ from nonces to which delegates commit during the cycle with the number $i-2$. One out of every BLOCKS_PER_COMMITMENT = 32 blocks can contain a commitment. So, there are at most BLOCKS_PER_CYCLE / BLOCKS_PER_COMMITMENT = 128 commitments in each cycle (where BLOCKS_PER_CYCLE = 4096 blocks). A commitment is the hash of a nonce which is generated by the baker who produces the block and is included in the block header. The committed nonce must be revealed by the original baker during the cycle with the number $i-1$ under penalty of forfeiting the rewards and fees of the block that included the commitment. The associated security deposit is not forfeited.

A nonce revelation is an operation, and multiple nonce revelations can thus be included in a block. A baker receives a SEED_NONCE_REVELATION_TIP = 1/8 reward for including a revelation. Revelations are free operations which do not compete with transactions for block space. Up to MAX_REVELATIONS_PER_BLOCK = 32 revelations can be contained in any given block.

Thus, (BLOCKS_PER_CYCLE / MAX_REVELATIONS_PER_BLOCK) / BLOCKS_PER_COMMITMENT = 4 blocks in a cycle are sufficient to include all revelations. The seed for the cycle with the number i is obtained as follows: the seed of cycle with the number $i-1$ is hashed with a constant and then with each nonce revealed in cycle with the number $i-1$.

The grinding attack we propose is just based on this bakers' election procedure. Note that the endorsers election procedure is very similar, so the attack described bellow is also suitable for endorsers election.

Let an attacker that controls p-fraction of stake for some significant minority (say $p=0.1$) trying to grind on the nonce for the cycle i does the following.

- In the cycle with the number $i-2$, the average number of commitment-containing blocks to be attributed to adversary is $128p$ (i.e., he is elected as the highest-priority baker for these blocks). In each of these blocks, adversary includes commitments to random nonces just as the protocol prescribes.
- In the cycle with the number $i-1$, bakers of commitment-containing blocks from the cycle with the number $i-2$ are supposed to open their commitments and publish the underlying nonces that they committed to. Assuming that all other nonce-creators from the cycle with the number $i-2$ are honest, adversary will see their openings (and hence their nonces) soon after the start of cycle with the number $i-1$. Now he can decide which of his commitments are to be opened: if he created about $128p$ commitments in the cycle with the number $i-2$, he has about 2^{128p} possibilities to choose (for example, in the 10% example this is about 2^{13}). For each of these possibilities (as long as his computational capacities allow), adversary computes the resulting randomness seed for cycle with the number i+PRESERVED_CYCLES, and chooses the possibility that gives her the most highest-priority baking positions in that cycle.
- An adversary waits until the cycle with the number i+PRESERVED_CYCLES and uses the disproportional block-creating rights, either for executing the grinding attack again (just stronger), or for getting disproportional rewards for baking, or for some other attack like double-spending.

3. Probabilistic model of bakers election

Now we formalise the bakers election procedure and describe its probabilistic model. We will use this model below, in description and analysis of grinding attack on this procedure.

We need to introduce some designations. Let N is the number of blocks in each cycle, and n be the number of blocks with commitments. Let there exist L stakeholders whose stakes we will denote as $S_1,\dots,S_L$, where S_i is the stake of i-th stakeholder. Define their general stake as $S=S_1+\dots+S_L$. The probability to choose some stakeholder for baking of some block for the next cycle is proportional to the value of its stake. We assume that stake distribution has not being changed during the period of attack. We also assume that the election of baker for the next block is independent of its prehistory. More formally, when choosing bakers for the next cycle, we assume that the probability that j-th block will be baked by i-th stakeholder is equal to some constant $p_i=\frac{S_i}{S}$, $j=\overline{1,N}$, $i=\overline{1,L}$, which depends only on current stake S_i.

To describe formally the procedure of bakers election we will use the probabilistic model of sampling with replacement, which most accurately reflects the probabilistic characteristics of the procedure.

Probabilistic model of bakers election

Let us have a box with balls of L different colours, and the probability to take the ball of i-th colour is p_i. We take sequentially N balls (with returning). If on the j-th step, $j = \overline{1,N}$, we take the ball of the i-th colour, then the i-th stakeholder is the baker of j-th block.

Under the terms "one attempt" or "one trial" we will understand the event which is determined as choosing sequentially, with returning, X balls from the box, where X may take values N (in case of bakers election for all blocks in cycle) or n (when we consider bakers election only for blocks with commitments). Note that all such trials are independent.

In what follows we will assume that the common adversary's stake ratio is equal to p, and common stake ratio of all other (honest) stakeholders is $q = 1 - p$. In this case we can simplify our model to the case of two-coloured balls, say white and black, and the probability to take white or black ball is equal to p or q, respectively.

4. Probabilities of two variants of grinding attack

In this section we consider two variants of grinding attack. Both of them are two-steps attack and are different only in the second step.

Step 1. On this step adversary waits for opening of all others commitments and then decides, what variant of grinding is more profitable for him on the second step: to maximize the number of his blocks with commitments (purposing to increase the number of grinding trials in the second step) or to maximize the number of his blocks in the corresponding cycle.

Step 2, variant 1. If it is more profitable to increase his ratio in blocks with commitments, he opens corresponding commitments and uses grinding to maximize the number of nonce commitment blocks. (It may help him to increase the number of grinding trials in the next step, if he decides to continue the process).

Step 2, variant 2. If it is more profitable to increase his ratio in all blocks in the cycle, he opens corresponding commitments and uses grinding to maximize the number of his slots in the whole cycle.

Note that in the next section we will discuss the more general case of attack, which may last arbitrary number of steps. According to our calculations, adversary can increase the number of commitment blocks up to on 80-120% in 1-2 cycles with non-negligible probability. The probability to deviate for more than 80-120% drops dramatically, so there is no sense in more than 1-2 iterations. Thus, having 10% of the total stake and assuming that in Step 2 (variant 1) the adversary increased the number of his commitment blocks two times (from 12 to 24), on the next step he can increase the total number of his slots in the next cycle approx on 25% (from ~400 to ~500).

Lemma 1.

For $X \in \{n, N\}$ and $l \in \{0,1,\ldots,X\}$, $K \in N$, the probability P that at least in one out of K grinding trials, the number of black balls in sample of X balls is not less than l is equal to

$$P = 1 - \left(1 - \sum_{k=l}^{X} \binom{X}{k} p^k q^{X-k}\right)^K. \quad (1)$$

Proof.

To get formulas for probabilities of success of grinding attack, introduce some auxiliary designations.

Define a random variable $\xi = \xi(X)$ as the number of black balls in sample of X balls, $X \in \{n, N\}$. Note that the event $\{\xi(n) = k\}$ happened on the first step of attack means that

adversary has exactly $K = 2^k$ grinding trials to increase the number of his commitment blocks or the number of blocks in the whole cycle on the second step.

Also for $X \in \{n, N\}$ and $l \in \{0,1,\ldots,X\}$ define the event $A = A(X,l)$ as

$$A(X,l) = \{\xi(X) \geq l\}. \tag{2}$$

Then, define the event $B = B(X,l,K)$ as "at least in one out of K grinding trials the event $A(X,l)$ happened". Now the probability in formula (1) is just the probability of the event $B = B(X,l,K)$.

According to the probabilistic model of bakers election, introduced in Section 2, the random variable $\xi = \xi(X)$ has binomial distribution: $P(\xi(X) = k) = \binom{X}{k} p^k q^{X-k}$, and the probability of the event $A(X,l)$ is equal to

$$P(A(X,l)) = \sum_{k=l}^{X} \binom{X}{k} p^k q^{X-k}. \tag{3}$$

Using (2), the event $B(X,l,K)$ may be represented as

$$\neg(\neg B(X,l,K)) = \{\text{in all } K \text{ trials the event } \neg A(X,l) \text{ happened}\}.$$

Then

$$P(B(X,l,K)) = 1 - P(\neg B(X,l,K)) = 1 - (1 - P(A(X,l)))^K, \tag{4}$$

because all K trials are independent.

Substitution (3) into (4) completes the proof. □

Now we are ready to find the probability of the grinding attack.

Theorem 1.

Let in the cycle number i +PRESERVED_CYCLES the adversary tries to increase the number of his commitment blocks or blocks in whole cycle, using his commitments from the cycle number $i-2$.

Then the probability $P(B(X,l))$ of the event

$$B(X,l) = \{\text{in the cycle number } i \text{ +PRESERVED\_CYCLES adversary gets } l \text{ out of } X \text{ blocks}\}$$

is equal to

$$P(B(X,l)) = \sum_{k=0}^{n} \left(1 - (1 - P(A(X,l)))^{2^k}\right) \times \binom{k}{X} p^k q^{n-k}, \tag{5}$$

where p is adversary's stake ratio, $X \in \{n, N\}$.

Proof. Note that events $\{\xi(n) = k\}_{k=0}^{n}$, which may happen in the cycle number $i-2$, form the full group of events. Then according to composite probability formula and using Lemma 1, obtain:

$$P(B(X,l)) = \sum_{k=0}^{n} P\left(B(X,l) \,/\, \xi(n) = k\right) \times P(\xi(n) = k) =$$

$$= \sum_{k=0}^{n} \left(1 - \left(1 - P\left(A\left(X,l\right)\right)\right)^{2^k} \right) \times \binom{k}{X} p^k q^{n-k} \quad . \square$$

Substituting N or n instead of X in (5), we get two formulas for probabilities that adversary with stake ratio p managed to get not less than l blocks in whole cycle or not less than l commitment blocks, respectively, where $0 \le l \le X$.

5. Numerical results

Here we give two Tables with numerical results obtained according to formula (5) for $X = n = 128$ (Table 1) and $X = N = 4096$ (Table 2).

Table 1. Probability that adversary with stake ratio p managed to get l or more commitment blocks in cycle i+PRESERVED_CYCLES, using his commitments from cycle $i-2$ (for $X = n = 128$)

l / p	0.1n=12	0.15n=19	0.2n=25	0.25n=32	0.3n=44	0.35n=44	0.4n=51	0.45n=57	0.5n=64
0.1	0.999994	0.996895	0.810652	0.053589	9.54E-05	1.57E-08	5.2E-16	6.2E-21	2.7E-27
0.15	1	1	0.999995	0.996898	0.831635	0.157741	0.000369	9.12E-08	5.2E-19
0.2	1	1	1	1	0.999995	0.998135	0.80569	0.144884	0.000337
0.25	1	1	1	1	1	1	0.999989	0.995971	0.712103
0.3	1	1	1	1	1	1	1	1	0.999953
0.35	1	1	1	1	1	1	1	1	1
0.4	1	1	1	1	1	1	1	1	1
0.45	1	1	1	1	1	1	1	1	1
0.5	1	1	1	1	1	1	1	1	1

Table 2. Probability that adversary with stake ratio p managed to get l or more blocks in whole cycle i+PRESERVED CYCLES, using his commitments from cycle $i-2$ ($X = N = 4096$)

l / p	0.1n=409	0.15n=614	0.2n=819	0.25n=1024	0.3n=1228	0.35n=1433	0.4n=1638	0.45n=1843	0.5n=2048
0.1	0.999986	6.25E-20	1.8E-77	8.4E-163	3.6E-272	3.6E-403	1.4E-553	1.4E-721	1.4E-908
0.15	1	1	3.13E-14	1.1E-58	1.1E-127	3.2E-217	3.2E-326	3.2E-454	8.2E-600
0.2	1	1	1	0.000048	5.5E-50	1.3E-108	2.8E-187	5.7E-285	5.7E-399
0.25	1	1	1	1	0.0508	7.4E-46	1.3E-98	2.2E-170	3.3E-260
0.3	1	1	1	1	1	0.58	3.5E-44	4.8E-94	6.3E-161
0.35	1	1	1	1	1	1	0.962	6.2E-45	2.8E-92
0.4	1	1	1	1	1	1	1	0.999154	8.6E-47
0.41	1	1	1	1	1	1	1	1	1.8E-40
0.42	1	1	1	1	1	1	1	1	7.9E-34
0.43	1	1	1	1	1	1	1	1	5.08E-29
0.44	1	1	1	1	1	1	1	1	0.9589
0.45	1	1	1	1	1	1	1	1	0.999993
0.5	1	1	1	1	1	1	1	1	1

According to Table 2, we can conclude that to get not less than a half of blocks in a whole cycle in simple two-step grinding attack adversary should have stake ratio about 0.44. With smaller stake rate such event has negligible probability.

6. A few words about generalisation of grinding attack

Now let's get back to the generalization of the attack, mentioned in Section 4.

This generalization is as follows. After Step 1, the attacker makes several iterations corresponding to variant 1 of Step 2, gradually increasing his share among the blocks with commitments. Having increased it to the desired value, he goes to variant 2 of Step 2 and tries to get at least half of all the blocks of the next cycle. Is this generalised attack significantly more effective than the simpler one, discussed earlier? And does it make sense to do many iterations aimed at increasing the number of blocks with commitments? Will it help the adversary to get half or more blocks in a whole cycle?

Let us try to answer these questions. Suppose that the attacker, as a result of iterative execution of variant 1 of Step 2, managed to obtain all 128 blocks with commitments. Also make an assumption in favour of the attacker and suppose that his computational abilities are sufficient to enumerate all 2^{128} options for opening commitments (although this is hardly possible without a quantum computer). We won't build something like Tables 1 and 2 with large volume of calculations, but only estimate the probability $P\left(B\left(4096,2048,2^{128}\right)\right)$ that an attacker with a stake ratio p will be able to get more than half of all blocks of the corresponding cycle, if in the previous cycle he received all the blocks with commitments. Also we estimate the minimal stake ratio for which such probability is significant.

According to our previous results,

$$P\left(B\left(4096,2048,2^{128}\right)\right)=1-\left(1-P\left(A\left(4096,2048\right)\right)\right)^{2^{128}}, \tag{6}$$

where

$$P\left(A\left(4096,2048\right)\right)=\sum_{k=2048}^{4096}\binom{4096}{k}p^k q^{4096-k}. \tag{7}$$

The problem is to calculate (6) and (7) with sufficient accuracy.

First of all note that $2^{128}\approx 10^{38,8}<10^{39}$. Then, if $P\left(A\left(4096,2048\right)\right)<10^{-41}$, we can approximate (6) as

$$P\left(B\left(4096,2048,2^{128}\right)\right)\approx 10^{39}\cdot P\left(A\left(4096,2048\right)\right) \tag{8}$$

where calculation error isn't larger than $\left(10^{39}\cdot P\left(A\left(4096,2048\right)\right)\right)^2<10^{-4}$.

Next, note that $P\left(A\left(4096,2048\right)\right)$ increases with increasing stake ratio p. As for $p=0.39$ we get $P\left(A\left(4096,2048\right)\right)\approx 2.6\cdot 10^{-46}$, then we can use approximation (6) for all stakes which are not large than 0.39.

Using (6) for $p=0.39$, we get negligible small probability

$$P\left(B\left(4096,2048,2^{128}\right)\right)\approx 10^{39}\cdot 2.6\cdot 10^{-46}=2.6\cdot 10^{-7},$$

which allows us to conclude that for smaller stake ratios probabilities of such events will also be negligible.

For $p=0.4$ we get

$$P\left(A\left(4096,2048\right)\right)\approx 1.8\cdot 10^{-38},$$

so in this case we can't apply approximation (8).

Calculating expression in right part of (6) directly for $p=0.4$ we get

$$P\left(B\left(4096,2048,2^{128}\right)\right)\approx 0.99999999999999,$$

which is indistinguishable from 1.

Based on these numerical results we can conclude that generalisation of grinding attack, aimed to obtain a half or more blocks in a whole cycle, doesn't work when adversary's stake ratio isn't large than $p=0.39$, even in case if he was lucky to get all commitment blocks in some cycle.

7. Conclusions

We proposed and analyzed two versions of grinding attack on bakers election procedure in Tezos protocol, in which adversary tries to increase his ratio of blocks with commitments or of blocks in the whole cycle. We show that even in the best case for the adversary he need at least about 40% of whole stake to succeed in this attack. But on the other hand, the adversary with stake ratio about 44% can easily capture half of all blocks in the cycle with probability close to 1, having significantly smaller stake ratio.

The further research may take into consideration more general view on the whole consensus protocol properties for rational participants: economic implications of not opening commitments as well as involving endorsers in the analyzed model for improved attacks.

REFERENCES

[1] Tezos — a self-amending crypto-ledger. White paper, 2014. URL: https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf

[2] Proof-of-Stake in Tezos. Tezos Developer Resources. URL: https://tezos.gitlab.io/009/proof_of_stake.html

[3] Tezos. GitLab. URL: https://gitlab.com/tezos/tezos

[4] E. Deirmentzoglou, G. Papakyriakopoulos and C. Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols," in IEEE Access, vol. 7, pp. 28712-28725, 2019, doi: 10.1109/ACCESS.2019.2901858.

к.т.н. Бєляков Р.О. (ВІТІ ім. Героїв Крут)
д.т.н. Романюк В.А. (ВІТІ ім. Героїв Крут)

МЕТОД МАРШРУТИЗАЦІЇ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО АЛГОРИТМУ НАВЧАННЯ В FANET

Актуальність. Згідно досвіду розвинутих у військовому відношенні країн світу перспективна архітектура мобільної компоненти (МК) тактичної ланки управління буде неоднорідною, ієрархічною та включатиме три основні рівні [1], що включає повітряну комунікаційну мережу – FANET (Flying Ad hoc Network). Основною задачею мережі FANET є забезпечення зв'язності із наземними мережами. Завдяки мобільності, оперативності, адаптації швидкості і висоти польоту, телекомунікаційні аероплатформи (ТА) можуть ефективно доповнювати існуючі наземні мережі зв'язку. Застосування ТА дозволяє будувати нову наземно-повітряну архітектуру систем радіозв'язку військового призначення, однак потребує вирішення системою управління мережею множини задач планування і оперативного управління: тривимірного розгортання ТА; розрахунку часу і траєкторії польоту; управління топологією, забезпечення маршрутизації і заданої якості інформаційного обміну тощо.

Одним із завдань управління наземно-повітряною мережею є *управління маршрутизацією*, з метою здійснення побудови та підтримки маршрутів передачі корисної інформації заданої якості при виконані вимог до їх функціонування (мінімізації службового трафіку, зменшення витрат енергії батарей). Для реалізації завдань оперативного управління необхідно забезпечити виконання **мережевих цілей управління рівнем FANET** ієрархічної комунікаційної мережі, до яких можна віднести оптимум наступних параметрів $F_i = \{F_1, F_2, \ldots, F_n\}$:

F_1 – час розгортання мережі;
F_2 – енергетична ефективність вузлів мережі;
F_3 – ступінь покриття території (визначених районів);
F_4 – структурна надійність мережі;
F_5 – розподіл ресурсів ТА;
F_6 – час функціонування мережі;
F_7 – обсяг службового трафіка;
F_8 – час відновлення мережі;
F_9 – час побудови та підтримки маршрутів передачі даних заданої якості і т.д.

Проаналізувавши цільові функції управління повітряною комунікаційною мережею FANET можна відзначити, що розробка протоколу маршрутизації адаптованого під воєнні цілі із організації зв'язку, дозволить напряму або безпосередньо оптимізувати параметри F_i, тому розробка методу маршрутизації в мережах FANET є актуальним науковим завданням.

Постановка задачі: Необхідно проаналізувати існуючі методи (протоколи) маршрутизації, що використовуються в FANET, визначити функціональні залежності задачі маршрутизації в повітряних комунікаційних мережах, та описати ключові етапи нового методу маршрутизації на основі нейромережевого алгоритму навчання в FANET.

Аналіз останніх публікацій. Раніше запропоновані підходи пропонували здійснювати оптимізацію визначених мереж за одним або декілька показниками [4–7]. Так в [4] запропоновано управляти витратами енергії батарей, в [5] здійснювати багатокритеріальну оптимізацію маршруту с врахуванням його мобільності, в [6-8] оптимізувати топологію мережі за декількома показниками, в [8] враховувати тип трафіка. В дослідженнях [9-12] пропонуються евристичні протоколи маршрутизації, або удосконалені існуючі класичні протоколи [13, 14], однак у запропонованих рішеннях реалізовані лише аналітично-обґрунтовані алгоритми і глобальні оптимізаційні рішення що не можуть бути застосовані в реальних умовах. З метою вирішення згаданої вище проблематики науковцями почали розроблятися, і згодом активно

використовуватись протоколи маршрутизації на основі алгоритмів машинного навчання із підкріпленням RL (Reinforcement Learning), що набули своєї актуальності через порівняно просту практичну реалізацію [15–16]. У статті [17] проаналізовано протокол GPSR та його модифікації і запропоновано протокол DSEGR для розв'язання проблем: гнучкого енергетичного менеджменту, управління мережею, масштабованості, збільшення швидкості навчання, адаптованості до великих мереж, усунення затримок інформаційного обміну, вирішення питань зациклення маршрутів тощо. Проте, слід зазначити, що протокол DSEGR все ж має недоліки, що стосуються його практичної реалізації, а саме: для навчання повітряної мережі в [17] було застосовано 40 – 150 ТА, що протирічить обмеженням застосування повітряної комунікаційної мережі FANET (кількість ТА – для тактичного рівня (6 – 10)). Також, через високу динамічність вузлів наземної мережі, і велику швидкість ТА (швидкість безпілотника літакового типу в середньому складає ≈50 м/с), застосування класичних протоколів маршрутизації недоцільне, тому що вони не враховують тривімірний простір що може бути вирішене за рахунок "інтелектуальної" адаптації.

Традиційні протоколи маршрутизації, що застосовуються в мережах FANET умовно можна поділити на 4 групи:

Таблиця 1

Традиційні протоколи маршрутизації в мережах FANET

	Назва класу	**Приклад**	**Переваги**	**Недоліки**
1	Проактивні протоколи	OLSR (Optimized Link State Routing Protocol)	Містить інформацію про фактичний стан вузлів мережі	Велика кількість службової інформації; Необхідність частого оновлення таблиць маршрутизації
2	Реактивні протоколи	AODV (Ad hoc On-Demand Distance Vector)	Вибір маршруту здійснюється найкоротшим шляхом по запиту (дистанційно-векторний алгоритм), низька витрата трафіку у разі передачі заздалегідь встановленими маршрутами	Збільшується час пошуку альтернативного маршруту при збоях мережі
3	Гібридні протоколи	ZRP (Zone Routing Protocol)	Переваги проактивних та активних протоколів Зниження витрат на управління "довгими" маршрутами Усунення затримок передачі повідомлень в межах "своєї" зони	Збільшується обчислювальна складність, знижується енергоефективність в мережах із малою вузловою щільністю
4	Протоколи на основі ГССН (географічні)	GPSR (Geographic Perimeter Stateless Routing)	Немає необхідності збору таблиць маршрутизації, а вибір маршруту здійснюється найкоротшим шляхом за географічним положенням вузла адресата	У випадку потрапляння на пусту область велика витрата часу на пошук альтернативного маршруту передачі повідомлень (затримки), відсутність можливості енергетичного менеджменту

У статті [17] проаналізовано протокол GPSR та його модифікації QGEO (Q-learning-based geographic routing protocol), QNGPSR (Q-network enhanced GPSR protocol), TQNGPSR (traffic-aware QNGPSR), та FEQSEI (Q-routing algorithm with simulated annealing interference), і запропоновано протокол DSEGR (Deep-Reinforcement Learning-Based Geographical Routing protocol). Автори підкреслюють, що даний протокол вирішує всі проблемні питання присутні у повітряних мережах (табл. 2 [17]), а саме проблеми: гнучкого енергетичного менеджменту, управління мережею, масштабованості, адаптованості до різного типу задач, збільшення швидкості навчання, адаптованості до великих мереж, усунення затримок інформаційного обміну, вирішення питань зациклення маршрутів.

Таблиця 2

Протоколи маршрутизації на основі RL (Reinforcement Learning) в мережах FANET

Протокол маршрутизації	**Управління енергоресурсом**	**Управління атрибутами посилань (Hello packet)**	**Управління навантаженням мережі**	**Швидка адаптація в динамічному середовищі**	**Адаптація до масштабованості мереж**	**Мережі в яких реалізовано**
GPSR	-	-	-	+	+	MANET
QGEO	-	+	-	-	_	Mobile robot networks
QNGPSR	-	-	+	+	+	UANET
TNGPSR	-	-	+	+	+	UANET
FEQSAI	+	+	-	+	-	FANET
DSEGR	+	+	+	+	+	UANET

Результат застосування запропонованого протоколу в [17] показав підвищену продуктивність з точки зору швидкості доставки пакетів.

В дослідженні [17] кожен Unmanned arial vehicle (UAV) виступав агентом, що дозволило скоротити час обміну статистичними вибірками станів вхідних даних на основі 200 епізодів (фаза 1, 2 алгоритму [17]). Завдяки великій надмірності агентів вдалося вибрати стратегію навчання нейромережі (фаза 3 [17]), і оптимальну політику винагород (фаза 4 [17]) для прийняття рішення із вибору маршруту. Підсумовуючи вище зазначене, можна зробити висновок, що реалізація запропонованого протоколу із урахуванням ресурсних обмежень (кількість UAV) буде ускладнена, а час розгортання і навчання агентів суттєво збільшиться. Так, моделювання здійснено для швидкостей 1 – 20 м/с, що накладає обмеження на тип безпілотників (можливість застосування лише для коптерного типу). Збільшену кількість UAV застосованих в дослідженні можна пояснити тільки потребою подальшої масштабованості мережі [17].

Крім того, навчання мережі на основі запропонованого протоколу повинно здійснюватися завчасно, що не представляється можливим в реальних умовах застосування мобільних ієрархічних багаторівневих мереж військового призначення.

Пропонується новий підхід – на етапі навчання вузлів повітряної мережі і прийняття рішення щодо реалізації задач маршрутизації в мережі FANET застосувати нейромережевий алгоритм машинного навчання, з метою адаптації до вимог та обмежень присутніх в ієрархічних комунікаційних мережах військового призначення, та інтелектуалізувати процес оперативного управління повітряною комунікаційною мережею.

Виклад основного матеріалу.

Постановка задачі на розробку методу маршрутизації на основі нейромережевого алгоритму навчання в FANET.

Нехай мережа представлена направленим графом $G = (V, C)$, де $V = \{v_n\}, n = \overline{1,N}$ – множина випадково розташованих вузлів та $C = \{c_j\}, j = \overline{1,J}$ – множина каналів. Кожен вузол

має координати розташування P_i, топологія мережі $NTOP = \{NTOP_1, NTOP_2, \ldots, NTOP_N\}$ визначається на етапі навчання мережі, ТА на етапі навчання рухаються на визначеній площі $Q^2 \leq Q^2_{max}$, довільною траекторією *m* на визначеній висоті *h*.

Задані параметри стану інформаційного напрямку: кількість вузлів (ТА) FANET – десятки вузлів; радіоканали симетричні і напівдуплексні; тип інформації – $\xi = \overline{1,3}$, де 1 – відео, 2 – мова, 3 – дані; маршрутизація зондова, кординатна, один до одного; $g_i^{\xi}(t) \leq g_{imax}^{\xi}$ – інтенсивність вхідних потоків на вході *i*-го вузла; $W_i(t) \leq W_{imax}$ – інтенсивність зміни радіозв'язності із сусідніми вузлами; $s_{ij}(t) \leq s_{ijmax}$ – пропускна спроможність каналу; радіозв'язність між вузлами мережі підтримується одним з протоколів канального рівня; t_s^{ξ}, $\xi = \overline{1,3}$ – час затримки передачі повідомлень ξ-типу.

Нехай загальна кількість вузлів на деякому маршруті *m* рівна *k*. Кожен *i*-й вузол на маршруті живиться від акумуляторної батареї, яка характеризується деякою залишковою ємністю батареї $E_i(t)$ і визначає час "життя" *i*-го вузла T_i – тобто час, протягом якого цей вузол зможе передавати інформацію або приймати участь у її ретрансляції на маршруті *m*.

Час існування діючого маршруту T_m не повинен визначатися мінімальним часом „життя" *i*-го вузла T_{imin} на маршруті *m*.

Час "життя" *i*-го вузла визначається:

$$T_{gi} = \frac{E_i(t)}{\sum_{j=1}^{J} R_j(t)}, j = \overline{1,J},$$

де $E_i(t)$ – залишкова ємність батареї *i*-го вузла після відправки або ретрансляції деякого *j*-го пакету; $R_i(t)$ – коефіцієнт витрати енергії *i*-им вузлом при передачі *j*-го пакету, який обчислюється з виразу.

Множина вимог до методу маршрутизації $\{B_q\}$, $q = \overline{1,3}$: мінімальна завантаженість мережі службовою інформацією; можливість одночасного використання кількох метрик пошуку маршруту; робота в умовах децентралізованого управління; мінімальний час побудови маршруту; можливість передачі інформації кількома маршрутами; забезпечення заданої якості обслуговування QoS.

Допущення: потужність сигналу на прийомі та співвідношення SNR та кількість енергії витраченої на передачу одного пакету $E_{ji}(t) = const$ вважатимемо незмінними. Похибка визначення координат ТА не впливає на процес навчання та інформаційного обміну.

Необхідно: здійснити синтез методу маршрутизації на основі нейромережевого алгоритму навчання в FANET, який передбачав би фазу побудови нових та фазу підтримання діючих маршрутів передачі заданої якості на інформаційному напрямку між відправником *a* та адресатом *b*.

Етапи реалізації методу маршрутизації на основі нейромережевого алгоритму навчання в FANET.

1. Етап збору даних власного стану ТА.

Кожна ТА записує власну інформацію про місцезнаходження у час отримання останніх 5 моментів передачі hello-пакетів сусідніми ТА *i*, та зберігає їх у заголовку власного hello - пакету. Вузол *j* отримує послідовність місцезнаходження

$$P_i = [P_i(t_1), P_i(t_2), P_i(t_3), P_i(t_4), P_i(t_5)]. \quad (2)$$

Взаємне розміщення у двовимірному просторі (*x*, *y*) визначається за виразом

$$D_{j,i}(t_1) = \sqrt{\left(P_j^x(t_1) - P_i^x(t_1)\right)^2 + \left(P_j^y(t_1) - P_i^y(t_1)\right)^2}. \quad (3)$$

Відповідно інформація про відстані між j та i визначається кортежом

$$D_{j,i} = [D_{j,i}(t_1), D_{j,i}(t_2), D_{j,i}(t_3), D_{j,i}(t_4), D_{j,i}(t_5)]. \quad (4)$$

З метою забезпечення управління витратами енергії кожна ТА записує власну послідовність залишкової енергії в період останніх 5 моментів (прийом і передача) hello-пакетів сусідів *i* та формує кортеж значень залишкової енергії

$$E_i = [E_i(t_1), E_i(t_2), E_i(t_3), E_i(t_4), E_i(t_5)]. \quad (5)$$

Прогнозування залишкової енергії (заряд АКБ ТА) для вибору наступного адресата може проводитися із використанням моделі ARIMA, проте в такому випадку необхідно буде збільшити вибірку значень залишкової енергії до 10.

2. Етап побудови маршрутів між сусідніми вузлами.

Таким чином на першому етапі ТА обмінюються із сусідніми ТА hello-пакетів, в результаті формуючи таблиці топології із сусідніми (neighbor) вузлами

$$NT_j = \{x \in N_{nbr}(j) | (LS_{j,x}, E_x^{pre}, P_{x}, NTOP_x)\}, \quad (6)$$

де $LS_{j,x}, E_x^{pre}, P_{x}$ – параметри, що описують якість радіозв'язку між вузлом *j* та його сусіднім вузлом *x*, $NTOP_x$ – кортеж відстаней від вузла *x* до сусідніх вузлів. До переданих пакетів додається адресу джерела, та останнього перехідного вузла, для боротьби із зацикленнями.

3. Етап прогнозування якості маршрутів.

Навчання агентів (ТА) представимо як Марківський процес $\langle B, A, I_s, R_{j,x} \rangle$, де B – простір станів, I_s – ймовірності переходів із одного стану в інший, в наслідок A дій, $R_{j,x}$ – нагорода після переходу в інший стан. Тобто в загальному вигляді це відповідає сценарію, коли ТА після прийому пакету, для його передачі приймає рішення щодо вибору сусіднього ТА для передачі пакету наступним чином:

3.1. Простір станів:

$$B = \{b_1, b_2, \ldots, b_N\}, \quad (7)$$

де *N* – кількість ТА.

Відповідно, кожну ТА можна представити

$$B_j = \{x \in N_{nbr}(j) | (LS_{j,x}, E_x^{pre}, D_{j,k}, D_{x,k}, C_{j,x \to x,k}, D_{sum})\}, \quad (8)$$

де $D_{j,k}$ – відстань від вузла (ТА) *j* до кінцевого вузла *k*; $D_{x,k}$ – відстань від сусіднього вузла *x* до *k*; $C_{j,x \to x,k}$- вектор переходу; D_{sum} – параметр подвійного переходу.

3.2. Простір дій:

$$A = \{a_1, a_2, \ldots, a_N\}. \quad (9)$$

Дією вузла *j* буде вибір сусіднього вузла *x* для переходу: $a_j \in \{x | x \in N_{nbr}(j)\}$.

3.3. Ймовірність переходу станів:

Ймовірність переходу станів I_s має випадковий характер і визначається середовищем.

3.4. Функція винагороди:

Метою застосування функції винагороди R є забезпечення швидкої збіжності. Функція винагороди вузла *j* і сусіднього вузла *x*:

$$R_{j,x} = \begin{cases} 100, \text{ якщо } x - \text{вузол призначення (кінцевий)}; \\ -w_1 D_{x,k} + w_2 E_x^{pre} - w_3 PS_{j,x}, x - \text{проміжний вузол}, \end{cases} \quad (10)$$

де w_1, w_2, w_3 – вагові коефіцієнти відстані від *x* до *k*, прогнозованої залишкової енергії вузла *x*, і стійкість зв'язку між *j* та сусіднім *x* відповідно.

4. Етап донавчання та підтримання маршрутів.

На даному етапі вибирається нейромережевий алгоритм навчання, з метою інтелектуалізації процесу прийняття рішення щодо вибору вузла призначення відповідно до заданих умов (вихідних даних та критеріїв). В статті визначено три метрики – енергетична ефективність, якість радіозв'язку, та відстань.

Суть представленого авторами методу DSEGR [17] на етапі навчання та підтримання маршрутів полягає у виборі лінійної нейронної мережі в якості агента з алгоритмом зворотнього поширення помилки для пошуку оптимальної політики з наступними гіпер – параметрами:

- структура нейромережі складається з чотирьох рівнів нейронів {5×16×4×1}, (1-ший вхідний, 2-гий та 3-тій прихований, 5-тий вихідний;
- функція активації нейронів Scaled Exponential Linear Units (SELU) математична інтерпретація представлена нижче:

$$Selu(x)\begin{cases} f(x) = \lambda x, & x > 0; \\ f(x) = \lambda\alpha(e^x - 1), & x \le 0, \end{cases}$$

де λ, α - коефіцієнти нормування для поточних даних (λ ≈1.050700987193349852946, α ≈1,67326324235437728481);

- оптимізатор (алгоритм мінімізації цільової функції) модифікація алгоритму градієнтного спуску Adam;
- швидкість навчання 0,001;
- розмір пакету даних дорівнює 32.

В роботі [17] показано проблему неоднорідності кожної функції відповідно вище зазначених критеріїв, а саме, вплив зміни швидкості руху різних вузлів (БПЛА) на середню затримку ТА-ТА, вплив на коефіцієнт доставки пакетів та вплив на час першого втраченого вузла. Ці процеси відбуваються за різний часовий проміжок тому відповідно кожна окрема цільова функція обчислюються за допомогою методу нормалізації Min-Max, що може знижувати швидкість збіжності в процесі адаптивного навчання алгоритму DSEGR. Також, необхідно зазначити, що швидкість збіжності навчання алгоритму використаного для навчання агентів DDQN (Double Deep Q-learning Network), істотно залежить від пропорційного збільшення кількості (ТА) {40…150}, тому застосування DSEGR в реальному часі мережі FANET не є доцільним із урахуванням обмежень пред'явлених вимог щодо кількості ТА тактичного рівня $\cong 10$.

Відповідно щоб уникнути вище зазначених недоліків на 4-тому етапі донавчання та підтримання маршрутів в реальному часі під час оновлення hello-пакетів пропонується застосувати один із модифікацій алгоритму Extreme learning machine (ELM) такий як Forget Online Sequential Extreme learning machine (FOS-ELM), що визначає новизну запропонованого методу. Основна ідея алгоритму FOS-ELM полягає у можливості обробляти статистику вхідних даних ТА, і враховувати закономірності їх зміни в реальному часі з мінімальними обчислювальними вимогами за схемою ТА(фрагмент)-ТА(фрагмент), шляхом обробки фіксованого або змінного розміру блоку даних, застосовуючи алгоритм рекурсивних найменших квадратів (RLS).

Робота алгоритму FOS-ELM складається з двох основних етапів: етапу ініціалізації та етапу послідовного донавчання.

4.1. Етап ініціалізації: на цьому етапі відбувається процес ініціалізації матриці вагових коефіцієнтів заданої структури нейромережі та параметрів зміщення нейронів відносно вибірки даних яка формується в реальному часі. Необхідно зауважити, що на відміну від класичних нейромережевих алгоритмів FOS-ELM може навчатись а реальному часі і не потребує

додаткового часу на збір необхідної розмірності вибірки даних. Основний математичний апарат роботи алгоритму представлений нижче в рівняннях:

$$\beta_0 = \boldsymbol{P_0 H_0 T_0}, \tag{11}$$

$$P_0 = \left(\boldsymbol{H_0^T H_0} + \frac{\mathbf{I}}{C}\right)^{-1}, \tag{12}$$

де β_0 – матриця вагових коефіцієнтів обробки даних в структурі нейромережі, H_0 – матриця прихованого рівня нейромережі, T_0 – цільовий вихідний рівень (вектор) нейромережі, P_0 –результат формування структури нейромережі на основі алгоритму оберненої матриці, H_0^T – транспонована матриця прихованого рівня, $\frac{\mathbf{I}}{C}$ – процес оновлення структури нейромережі в залежності від важливості з'єднань нейронів, **I** – одинична матриця, C – параметр регулювання для уникнення процесу виродженості матриці.

4.2. Етап послідовного донавчання: на цьому етапі відбувається адаптивний процес оновлення вихідних вагових коефіцієнтів матриці прихованих рівнів H_{k+1} в реальному часі що наведено в рівнянні:

$$\beta_{k+1} = \beta_k + P_{k+1} H_{k+1}^T (T_{k+1} - H_{k+1}\beta_k), \tag{13}$$

$$P_{k+1} = P_k - P_k H_{k+1}^T (I + H_{k+1} P_k H_{k+1}^T)^{-1} H_{k+1} P_k, \tag{14}$$

де $k+1$ – індекс який показує процес відбору k – тих вибірок вихідних даних за критерієм важливості тобто даних відмінних від нуля для зменшення надлишкових обчислювальних затрат.

Далі відбувається процес прогнозування цільових параметрів за допомогою коефіцієнта забування $\lambda \in (0, 1]$. Враховуючи параметр λ, представлено перетворення вище наведених рівняння (14) в модифікований вигляд:

$$P_{k+1} = \frac{1}{\lambda} P_k - P_k H_{k+1}^T (\lambda^2 + \lambda H_{k+1} P_k H_{k+1}^T)^{-1} H_{k+1} P_k. \tag{15}$$

Із рівняння видно, що коефіцієнт забування λ дозволяє зменшити вплив алгоритму з застарілих вхідних даних, що дозволяє зменшити обчислювальні затрати на пошук оптимальних параметрів нейромережі.

Висновок.

Таким чином, результат аналізу існуючих протоколів маршрутизації повітряних комунікаційних мереж FANET показав, що існуючі рішення не в повній мірі дозволяють вирішити проблеми побудови та підтримки маршрутів заданої якості в умовах високої мобільності, та обмеженого ресурсу часу та засобів.

Враховуючи цільові функції управління мережею, щодо процесу розгортання та забезпечення стійкості мережі FANET в динамічних умовах запропоновано застосування методу маршрутизації на основі нейромережевого алгоритму навчання в FANET, а саме на основі алгоритму FOS-ELM.

Основна відмінність в порівнянні з традиційними нейромережевими алгоритмами навчання полягає в суттєвому збільшенні швидкості процесу навчання. Процес обчислення та параметризації моделі нейромережі FOS-ELM відбувається за допомогою інверсної матриці і не використовує ітеративне налаштування параметрів, що дозволяє здійснювати інтелектуальну підтримку діючих маршрутів в реальному часі.

Також, суттєвою перевагою застосування методу, на відміну від існуючих, є уникнення додаткових обмежень фізичного і програмного рівнів внаслідок відсутності потреби формувати статистичну вібірку вхідних даних, може "донавчатись" в реальному часі.

Використання запропонованого методу на основі алгоритму екстремального навчання на відміну від методів на основі традиційних нейромережевих алгоритмів, дозволить забезпечити підтримку маршруту шляхом прогнозування стану радіоканалів через ретранслюючі вузли для

побудови альтернативних обхідних маршрутів передачі даних заданої якості, що призведе до скорочення обсягів службового трафіка при локальному зондуванні.

Напрямком подальших досліджень є дослідження розробленого методу при різних розмірностях мережі, динаміки змін топології, умовах її функціонування, типів ТА, та їх обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Романюк В. А. Мережі MANET – основа побудови тактичних мереж зв'язку // *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення* : IV Науково-практичний семінар ВІТІ. К.: ВІТІ НТУУ "КПІ". 2007. С. 15–28.

2. Самоорганизующиеся радиосети со сверхширокополосными сигналами / [С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк]. – К.: НПП „Издательство „Наукова думка" НАН Украины". – 444 с.: ил.

3. Миночкин А. И., Романюк В. А. Методология оперативного управления мобильными радиосетями // Зв'язок. 2005. № 2. С. 53–58.

4. Olascuaga-Cabrera J. G., Lopez-Mellado E., Mendez-Vazquez. A multi-objective PSO strategy for energy-efficient ad-hoc networking // *IEEE Cybernetics Systems* : Man (SMC) Conference. 2011.

5. Babaei H., Romoozi M. Multi Objective AODV Based On a Realistic Mobility Model // IJCSI International Journal of Computer Science Issues. Vol. 7, Issue 3. No 3. May 2010.

6. Banner R., Orda A. Multi-Objective Topology Control in Wireless Networks // *IEEE INFOCOM* : Proceedings. 2008.

7. Selvi R., Rajaram R. Muliple-objective optimization of multimedia packet scheduling for ad hoc networks through hybridized genetic algorithm // The International Journal of Multimedia & Its Applications (IJMA). Vol.3, No.3. August 2011.

8. Романюк В. А. Цільові функції оперативного управління тактичними радіомережами // Збірник наукових праць ВІТІ НТУУ "КПІ". 2012. №1. С. 109–117.

9. Urquiza-Aguiar, L.; Tripp-Barba, C.; Igartua, M.A. A geographical heuristic routing protocol for VANETs. Sensors 2016, 16. P. 1567.

10.Yu Y., Ru L., Chi W., Liu Y., Yu Q., Fang K. Ant colony optimization based polymorphism-aware routing algorithm for Ad hoc UAV network. // Multimed. Tools Appl. 2016. Vol. 75. P. 14451–14476.

11.Zhao B., Ding Q. Route discovery in Flying Ad-hoc Network based on bee colony algorithm // *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)* 29–31 March : Proceedings. Dalian, China. 2019. P. 364–368.

12.Patel J., El-Ocla H. Energy efficient routing protocol in sensor networks using genetic algorithm // Sensors 2021. 2021. P. 7060.

13.Wu Q., Zeng Y., Zhang R. Joint trajectory and communication design for multi-UAV enabled wireless networks // *IEEE Trans. Wirel. Commun. 2018* : Proceedings. Vol. 17. P. 2109–2121.

14.Lin L., Sun Q., Wang S., Yang F. A geographic mobility prediction routing protocol for ad hoc UAV network // *2012 IEEE Globecom Workshops* : Proceedings. Anaheim, CA, USA. 3–7 December 2012. P. 1597–1602.

15.Arafat M. Y., Moh S. A Q-learning-based topology-aware routing protocol for Flying ad Hoc Networks // IEEE Internet Things 2022, 9. P. 1985–2000.

16.Liu J., Wang Q., He C., Jaffrès-Runser K., Xu Y., Li Z., Xu Y. Qmr: Q-learning based multi-objective optimization routing protocol for Flying Ad Hoc Networks // Comput. Commun. 2020. V. 150. P. 304–316.

17.Zhang Y., Qiu H. DDQN with Prioritized Experience Replay-Based Optimized Geographical Routing Protocol of Considering Link Stability and Energy Prediction for UANET. Sensors 2022. 2022. P. 5020. DOI: 10.3390/s22135020

18.Bieliakov R. O. Method of the intelligent system construction of automatic control of unmanned aircraft apparatus / R. O. Bieliakov, H. D. Radzivilov, O. D. Fesenko, V. V. Vasylchenko, O. G. Tsaturian, A. V. Shyshatskyi, V. P. Romanenko // Радіоелектроніка, інформатика, управління. 2019. № 1. С. 218–229.

19.Bieliakov R. Simulation of Platform-Free Inertial Navigation System of Unmanned Aerial Vehicles Based on Neural Network Algorithms // Technology audit and production reserves. 1 (2 (57)), 15-19. 2021. DOI: 10.15587/2706-5448.2021.225282

д.т.н. Горбенко І. Д. (ХНУ ім. В.Н. Каразіна, АТ "ІІТ")
к.т.н. Єсіна М. В. (ХНУ ім. В.Н. Каразіна, АТ "ІІТ")
к.т.н. Качко О. Г. (ХНУРЕ, АТ "ІІТ")
д.т.н. Олексійчук А.М. (НТУУ "КПІ")
к.т.н. Горбенко Ю.І. (АТ "ІІТ"))

ЗНИЖЕННЯ РИЗИКІВ ДЛЯ ВРАЗЛИВИХ КРИПТОГРАФІЧНИХ СИСТЕМ, РОЗРОБКА, СТАНДАРТИЗАЦІЯ ТА ВПРОВАДЖЕННЯ СТІЙКИХ ПОСТКВАНТОВИХ КРИПТОПРИМІТИВІВ НА МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ РІВНІ

Актуальність. За останні роки спостерігається стійкий прогрес у створенні квантових комп'ютерів. У разі реалізації великомасштабних квантових комп'ютерів вони будуть загрожувати безпеці багатьох широко використовуваних криптосистем з відкритим ключем. Схеми встановлення ключів і електронні підписи, засновані на факторизації, дискретних логарифмах і криптографії на еліптичних кривих (ЕК), найбільш сильно постраждають. Симетричні криптопримітиви, такі як блокові шифри і геш-функції, будуть порушені лише незначно Як результат, було проведено активізацію досліджень щодо пошуку криптосистем на відкритих ключах, які були б захищені від зловмисників як з квантовими, так і з класичними комп'ютерами. Цю область часто називають постквантовою криптографією (PQC), або іноді квантовостійкою криптографією. Мета полягає в розробці схем, які можна розгорнути в існуючих комунікаційних мережах та протоколах без суттєвих змін.

Постановка задачі. Об'єктом дослідження є процеси зниження ризиків для вразливих (існуючих) криптосистем, розробка, стандартизація та впровадження стандартизованих стійких постквантових криптопримітивів асиметричного шифрування (АСШ), електронного підпису (ЕП) та протоколів інкапсуляції ключів (ПІК) на міжнародному та національному рівнях.

Предметом досліджень є методи синтезу та методики оцінки, порівняльного аналізу та застосування нових доказовостійких національних та міжнародних стандартизованих криптопримітивів АСШ, ЕП та ПІК на міжнародному та національному рівнях.

Метою доповіді є:

- обґрунтування вибору, розробка та експериментальні дослідження сучасних та постквантових стандартизованих криптоперетворень АСШ, ПІК та ЕП для криптозахисту інформації в мережах зв'язку, надання користувачам мережі зв'язку послуг ідентифікації, автентифікації, цілісності, конфіденційності, доступності, неспростовності, криптоживучості та санкціонування кожному користувачу доступу в мережі зв'язку;
- аналіз стану процесів міжнародної стандартизації та умов впровадження асиметричної постквантової криптографії згідно 3-го етапу NIST США та проміжних постквантових та квантових досліджень Європейського союзу (ЄС);
- аналіз стану процесів національної стандартизації та умов і вимог щодо впровадження постквантової асиметричної криптографії в Україні, порівняльний аналіз постквантових національних та міжнародних стандартів та проектів стандартів АСШ, ЕП, ПІК згідно вимог щодо безпеки, продуктивності та експлуатаційних характеристик.

Основні положення

У відповідь на виклики, створені дослідженнями і розвитком у сфері квантових комп'ютерів, Національний інститут стандартів та технологій (NIST) ініціював відкритий конкурсний процес для вибору квантовостійких криптоалгоритмів. Нові стандарти криптографії з відкритим ключем визначатимуть алгоритми для ЕП, АСШ і ПІК. Передбачається, що ці алгоритми будуть здатні захистити конфіденційну інформацію в доступному для огляду майбутньому, в тому числі після появи квантових комп'ютерів.

NIST публічно оголосив про початок подання заявок до процесу стандартизації PQC у грудні 2016 року. До листопада 2017 року було подано 82 алгоритми-кандидати. Незабаром

після цього 69 кандидатів, які відповідали як вимогам подання, так і критеріями мінімальної прийнятності, були прийняті в першому раунді процесу стандартизації. Ці кандидати базувались на математичних методах на основі: алгебраїчних решіток, математичних кодів, ізогеній еліптичних кривих, одноразових ключів та багатовимірних перетворень [1].

Після багаторічного огляду кандидатів NIST вибрав 26 алгоритмів для переходу до 2-го раунду оцінки в січні 2019 року [2]. Ці алгоритми розглядалися як найбільш перспективні кандидати для можливої стандартизації і були обрані на основі як внутрішнього аналізу, так і відгуків спільноти. Після ретельного обговорення NIST вибрав 7 фіналістів та 8 альтернативних варіантів, щоб перейти до 3-го раунду в липні 2020 року [3]. Намір NIST полягав у стандартизації невеликої кількості фіналістів наприкінці 3-го, а також невеликої кількості альтернативних кандидатів після 4-го раунду.

Після трьох раундів оцінки та аналізу, NIST вибрав перші алгоритми, які він стандартизує в результаті процесу стандартизації PQC, а також алгоритми, які ще необхідно дослідити – вони будуть досліджуватись у 4-му раунді [4].

Окрім конкурсу NIST, проводиться і дослідження на квантово-стійкі криптоалгоритми на національному рівні. Вже запропоновані та знаходяться у роботі стандарти постквантових алгоритмів АСШ, ПІК та ЕП.

Також для протистояння квантовим комп'ютерам і загрозам, які вони за собою несуть, у США розроблено та прийнято «Меморандум про національну безпеку з просування лідерства США в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем» від 4 травня 2022 року. У меморандумі викладено політику та ініціативи адміністрації президента США, пов'язані з квантовими обчисленнями. У ньому визначено ключові кроки, необхідні для збереження конкурентної переваги країни в галузі квантової інформаційної науки, а також зниження ризиків, пов'язаних з квантовими комп'ютерами для кібер-, економічної та національної безпеки країни. У ньому вказані конкретні дії, які мають зробити відомства, оскільки США розпочинають багаторічний процес переведення вразливих комп'ютерних систем на квантово-стійку криптографію [5].

1. Вимоги NIST до кандидатів у постквантові криптоалгоритми

Під час проведення конкурсу NIST PQC, NIST було висунуто перелік вимог, яким повинні були відповідати кандидати на постквантові криптоалгоритми. Основними з них була відповідність визначеним рівням безпеки та відповідність визначеній моделі безпеки.

Рівні безпеки NIST США, яким повинні відповідати обрані криптопримітиви:

1 рівень – принаймні так важко зламати, як AES-128 (вичерпний перебір ключів).

2 рівень – принаймні так важко зламати, як SHA-256 (пошук колізії).

3 рівень – принаймні так важко зламати, як AES-192 (вичерпний перебір ключів).

4 рівень – принаймні так важко зламати, як SHA-384 (пошук колізії).

5 рівень – принаймні так важко зламати, як AES-256 (вичерпний перебір ключів).

NIST попросив заявників зосередитись на рівнях 1, 2, 3 (4 і 5 призначені для дуже високої безпеки).

Обрані криптопримітиви повинні відповідати визначеній моделі безпеки:

- для АСШ – в умовах дії моделі безпеки IND-CCA2 (Indistinguishability adaptive ciphertext attack), що визначає нерозрізнювальність при атаці на основі адаптивно підібраного шифртексту;

- для ЕП – в умовах дії моделі безпеки EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), що визначає екзистенційну непідроблюваність при атаці на основі вибраного повідомлення;

- для протоколу інкапсуляції ключів – в умовах дії моделі безпеки Canetti-Krawczyk (CK-безпека).

2. Відбір кандидатів NIST для стандартизації та подальших досліджень

Під час 3-го раунду було отримано деякі криптоаналітичні результати, які мали значний вплив на вибір NIST. Атака на GeMSS різко знизила його безпеку та підірвала впевненість NIST у ньому. Цей результат призвів до виключення GeMSS з розгляду для стандартизації NIST.

Алгоритм Rainbow також зазнав значних атак під час 3-го раунду [4]. Перша атака на початку 3-го раунду спричинила втрату наборами параметрів від 20 до 55 біт безпеки в моделі RAM, причому набори параметрів з вищим рівнем безпеки втрачали більше бітів безпеки. За цим послідувала більш серйозна атака наприкінці 3-го раунду, що призвела до відновлення особистого ключа для параметрів категорії безпеки 1 трохи більше, ніж за два дні обчислень на одному ноутбуці. Через брак впевненості в безпеці NIST не вибрав Rainbow для стандартизації.

NIST також вирішив вилучити FrodoKEM, NTRU Prime та Picnic з розгляду для стандартизації. FrodoKEM – це кандидат, заснований на решітці, якого було обрано як альтернативний варіант під час 2-го раунду. FrodoKEM в основному вирізняється тим, що він не покладається на структуровані решітки (на відміну від фіналістів Kyber, NTRU та Saber). У той час як NIST має намір вибрати принаймні один додатковий KEM, не заснований на структурованих решітках, для стандартизації після 4-го раунду, три інші альтернативи KEM (BIKE, HQC і SIKE) краще підходять для цієї ролі, ніж FrodoKEM. FrodoKEM загалом має гіршу продуктивність, ніж ці три, тому не розглядатиметься надалі для стандартизації. NTRU Prime також було висунуто як альтернативний варіант, оскільки він вважався менш перспективним порівняно з фіналістами. Під час 3-го раунду не було результатів, які б суттєво змінили цю точку зору. Оскільки NIST буде стандартизувати один із фіналістів KEM (на основі структурованих решіток), NTRU Prime не було обрано для продовження процесу. Схожа ситуація була і з підписами. Picnic не було обрано, оскільки NIST вирішив стандартизувати SPHINCS+. Picnic та SPHINCS+ мають подібні профілі ефективності (невеликі відкриті ключі та великі підписи) і підходять для тих же випадків використання. SPHINCS+ і Picnic мають кілька версій, що робить пряме порівняння витрат та ефективності більш складним. Однак у кожного з них є набагато більша вартість та набагато гірша продуктивність порівняно з Dilithium та Falcon, що робить ці критерії менш важливими. Безпека Picnic не краща, ніж у SPHINCS+, і NIST вважає, що, хоча SPHINCS+ є зрілою конструкцією, Picnic та пов'язані з ним схеми продовжуватимуть отримувати користь від майбутніх досліджень та вдосконалень.

Вибираючи між подібними алгоритмами KEM, вартість та ефективність були значними критеріями відбору [4].

Одним із важких виборів, з якими стикнувся NIST, було прийняття рішення між Kyber, NTRU та Saber. Усі троє були обрані фіналістами і були дуже порівнянні один з одним. NIST впевнений у безпеці, яку забезпечує кожен. Більшість додатків зможуть використовувати будь-яку з них без суттєвих штрафів на продуктивність. Як зазначається на завершення 2-го раунду, NIST мав намір стандартизувати лише один із цих фіналістів, оскільки всі троє базувалися на структурованих решітках. Проблеми, пов'язані з патентами, були фактором рішення NIST протягом 3-го раунду, оскільки NIST дізнався про різні сторонні патенти. Однією з відмінностей між Kyber, Saber та NTRU є конкретне припущення щодо безпеки, що кожен покладається на безпеку. NIST вважає проблему MLWE, від якої залежить Kyber, трохи переконливішою, ніж інші припущення, такі як MLWR або проблема NTRU. NIST також високо оцінив специфікацію команди Kyber, яка включала ретельний і детальний аналіз безпеки. Що стосується продуктивності, то Kyber був майже найкращим (якщо не найкращим) у більшості тестів [4].

Решту обраних кандидатів KEM (BIKE, Classic McEliece, HQC, SIKE) продовжуватимуть оцінювати у 4-му раунді. І BIKE, і HQC засновані на структурованих кодах і будуть придатними як KEM загального призначення, що не ґрунтується на решітках. NIST може вибрати максимум одного з цих двох кандидатів для стандартизації по завершенню 4-го раунду. SIKE залишається привабливим кандидатом для стандартизації через його невеликі розміри ключа та шифртексту.

NIST сподівається, що подальше вивчення SIKE триватиме протягом 4-го раунду. Classic McEliece був фіналістом, але наразі не стандартизується NIST. Хоча він вважається захищеним, NIST ще не передбачає, що він буде широко використовуватись через великий розмір відкритого ключа [4].

NIST мав намір вибрати щонайменше одного з Dilithium та Falcon, оскільки обидва базуються на структурованих решітках і можуть використовуватися в більшості додатків. Зрештою, NIST вирішив вибрати обидві схеми для стандартизації. Генерація ключа та підпису для Falcon, схоже, потребує більшої кількості ресурсів (гейтів та RAM), ніж Dilithium, що може зробити Falcon непридатним для впровадження на обмежених пристроях, особливо у випадках, коли вимагається захист від атак бічними каналами. Крім того, NIST визнає, що простіша конструкція ключа та генерації підписів Dilithium допоможе забезпечити безпечні реалізації. З цих причин NIST вибрав Dilithium як основний алгоритм підпису, який він рекомендує для загального використання, і надасть пріоритет його стандартизації [4].

NIST розуміє, що деякі додатки не працюватимуть так, як вони були розроблені, якщо підпис та дані, що підписуються, не будуть вписуватися в один Інтернет-пакет. Для цих додатків складність реалізації генерації підпису Falcon може не викликати занепокоєння, але труднощі з модифікацією додатків для роботи з більшим розміром підпису Dilithium можуть створити бар'єр для переходу до постквантових схем підпису. З цієї причини NIST вирішив також стандартизувати Falcon. Враховуючи загальну кращу продуктивність Falcon, коли генерацію підписів не потрібно виконувати на обмежених пристроях, багато додатків можуть вважати за краще використовувати Falcon, ніж Dilithium, навіть у випадках, коли розмір підпису Dilithium не буде перешкодою для реалізації.

Для того, щоб не покладатися повністю на безпеку решіток, NIST також стандартизує SPHINCS+. Безпека алгоритму підпису SPHINCS+ добре зрозуміла, хоча він набагато більший та повільніший, ніж алгоритми підпису на решітках. NIST визнає, що SPHINCS+ може не підходити для багатьох додатків, враховуючи його профіль продуктивності. NIST зробив вибір вибрати SPHINCS+ зараз, замість того, щоб включити його в 4-й раунд. Таким чином, це означає кінець поточного процесу для схем підписів. Усі кандидати алгоритму підпису або були обрані для стандартизації, або видалені з розгляду для стандартизації. NIST може стандартизувати більше підписів у майбутньому, але це займе кілька років, і немає гарантій кращих алгоритмів.

Підводячи підсумок, NIST обрав чотири алгоритми з 3-го раунду для стандартизації та чотири алгоритми для просування до 4-го раунду для подальшої оцінки та вивчення [4].

Таким чином, у табл. 1 та 2 наводяться алгоритми, які слід стандартизувати та, які переходять до 4-го раунду, відповідно [4].

Таблиця 1 – Алгоритми, які слід стандартизувати

Шифрування на відкритому ключі/KEM	Цифрові підписи
Crystals-Kyber	Crystals-Dilithium
	Falcon
	SPHINCS+

Таблиця 2 – Кандидати, що переходять до четвертого раунду

Шифрування на відкритому ключі/KEM	Цифрові підписи
BIKE	
Classic McEliece	
HQC	
SIKE	

3. Квантово-захищені національні стандарти України

У той же час в Україні вже розроблені або знаходяться на стадії прийняття квантово-захищені криптографічні алгоритми. Всі вони наведені у таблиці 3.

Важливим загальним результатом наших досліджень та розробки є те, що прийняті наші рішення щодо вибору математичних основ побудови перспективних стандартів ЕП "Вершина" та "Сокіл" повністю співпали з подальшим рішеннями NIST США по закінченню 3-го раунду конкурсу NIST PQC на перспективні стандартні алгоритми електронного підпису, які були опубліковані раніше, ніж пропозиції NIST США. Проєкт стандарту ЕП "Вершина" використовує математичні засади Dilithium, а ЕП "Сокіл" – математичні засади Falcon.

Таблиця 3 – Квантово-захищені національні стандарти України

Існуючі стандарти	Проєкти стандартів (знаходяться у розробці)
ДСТУ 7624-2014 (Калина) – блокове симетричне шифрування	Проєкт ДСТУ (Вершина) – електронний підпис
ДСТУ 7564-2014 (Купина) – функція гешування	Проєкт ДСТУ (Сокіл) – електронний підпис
ДСТУ 8845-2019 (Струмок) – потокове шифрування	
ДСТУ 8961-2019 (Скеля) – асиметричне шифрування та інкапсуляція ключів	

Алгоритм ЕП "Вершина" може працювати у наступних режимах:

- Вершина-128/64 (нульовий) – 128 біт захисту від класичних атак та 64 біт від квантових атак, захист від спеціальних атак (запас стійкості ДСТУ 7624-2014 (128), AES (128));
- Вершина-256/128 (перший) – 256 біт захисту від класичних атак та 128 біт від квантових атак, захист від спеціальних атак (запас стійкості ДСТУ 7624-2014 (256), AES (256));
- Вершина-384/192 (другий) – 384 біт захисту від класичних атак та 192 біт від квантових атак, захист від спеціальних атак (запас стійкості ДСТУ 7624-2014 (512));
- Вершина-512/256 (третій) – 512 біт захисту від класичних атак та 256 біт від квантових атак, захист від спеціальних атак (запас стійкості ДСТУ 7624-2014 (512)).
- Вершина-*c* – для сумісності з режимом Dilithium (128, 256 біт).

У залежності від необхідного рівня безпеки та обмежень на техніко-експлуатаційні та техніко-економічні характеристики ЕП «Сокіл» може застосовуватись із забезпеченням 1, 2 та 3 рівнів безпеки та криптографічної живучості відповідно із забезпеченням 128, 256 та 512 біт безпеки проти класичного криптоаналізу та 64, 128 та 256 біт безпеки проти квантового криптоаналізу, а також із забезпеченням захисту від спеціальних атак.

Теоретична безпека ЕП «Сокіл» підтверджується доказом у моделі QROM на основі складності SIS над NTRU решітками.

Консервативні оцінки складності підробки ЕП «Сокіл» мають такі ж самі значення, як і для ЕП "Вершина".

Висновки

1. Основними алгоритмами, рекомендованими NIST для більшості випадків використання, є Crystals-Kyber (встановлення ключа) і Crystals-Dilithium (електронні підписи). Крім того, схеми підпису Falcon і SPHINCS+ також будуть стандартизовані. Кандидати BIKE, Classic McEliece, HQC і SIKE будуть продовжуватись вивчатись далі у 4-му раунді оцінювання.

2. 4-й раунд оцінювання та аналізу відбуватиметься подібно до попередніх раундів. Після завершення 4-го раунду NIST може вирішити вибрати деяких із кандидатів 4-го раунду для стандартизації.

3. В Україні також на національному рівні вже розроблені або знаходяться на стадії прийняття квантово-захищені криптографічні алгоритми. Серед вже розроблених такі стандарти: ДСТУ 7624-2014 (Калина) – блокове симетричне шифрування, ДСТУ 7564-2014 (Купина) – функція гешування, ДСТУ 8845-2019 (Струмок) – потокове шифрування, ДСТУ 8961-2019 (Скеля) – асиметричне шифрування та інкапсуляція ключів. Серед проектів стандартів: ДСТУ (Вершина) – електронний підпис, ДСТУ (Сокіл) – електронний підпис.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology (2016) NIST post-quantum cryptography standardization. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (дата звернення: 26.10.2022).

2. Alagic G. Status report on the first round of the NIST post-quantum cryptography standardization process / Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Liu Y. K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. // (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240. (2019). URL: https://doi.org/10.6028/NIST.IR.8240 (дата звернення: 26.10.2022).

3. Alagic G. Status report on the second round of the NIST post-quantum cryptography standardization process / Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Kelsey J., Liu Y. K., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. // (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8309. (2020). URL: https://doi.org/10.6028/NIST.IR.8309 (дата звернення: 26.10.2022).

4. Gorjan Alagic NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai, Liu Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // URL: https://doi.org/10.6028/NIST.IR.8413 (дата звернення: 26.10.2022).

5. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/ (дата звернення: 26.10.2022).

Нерознак Є.І. (ВІТІ імені Героїв Крут)
Ph.D Фесьоха В.В (ВІТІ імені Героїв Крут)
д.т.н. Сова О.Я. (ВІТІ імені Героїв Крут)

МЕТОД АДАПТИВНОГО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В КЛАСТЕРНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ РІВНОВАГИ НЕША

Актуальність дослідження. В умовах постійного зростання попиту на інформатизацію усіх сфер життєдіяльності суспільства залишається відкритим питання надійного та стабільного (неперервного) функціонування інформаційних систем/сервісів (ІС), що надають послуги користувачам у режимі реального часу. Так, за звітними даними кількість клієнтських запитів, зростає майже експоненціально, що унеможливлює вирішення даного питання шляхом постійного горизонтального та/або вертикального масштабування інформаційних систем в умовах обмеженості серврених ресурсів кластерних систем.

У даному контексті особливої уваги заслуговує стабільне (неперервне) функціонування ІС критичної інфраструктури держави, зокрема ІС військового призначення (сил оборони та безпеки), адже їх функціонування як у повсякденній діяльності, так і в умовах воєнного стану передбачають щоденне прийняття важливих для національної безпеки рішень, захисту територіальної цілісності України, управління військами, провадження антитерористичної та контрдиверсійної діяльності, збереження життя, прав і свобод громадян.

Одним з основних напрямків вирішення даного питання є підвищення продуктивності кластерних систем – апаратного фундаменту загального і спеціального програмного забезпечення, шляхом ефективного балансування навантаження між серверами кластерних систем з метою оптимального їх використання в умовах обмеження апаратних ресурсів та прийнятного часу на обробку запитів.

Це обумовлює актуальність подальших наукових досліджень щодо підвищення ефективності балансування навантаження кластерних систем військового призначення, спричиненого непередбачуваною зміною інтенсивності та/або важливістю (пріоритетністю) клієнтських запитів.

Аналіз наукових публікацій за даною тематикою показав доцільність застосування теоретико-ігрового підходу до вирішення вищевказаного питання. Дійсно, стратегії (діяльність) клієнтів (клієнтських запитів) є егоїстичними по відношенню один-до-одного (оптимізація власної продуктивності без узгодження з іншими), але, у той же час, залежать від стратегій інших учасників даного процесу і, як наслідок, впливають на результат навантаження кластерної системи в цілому, оскільки пов'язані з використанням та перерозподілом спільних ресурсів. Очевидно, що описана взаємодія є некооперативною грою, де гравці – клієнти (клієнтські запити), які намагаються мінімізувати очікуваний час відповіді власних завдань, а множина стратегій гри – сервери кластерної системи, до яких спрямовані клієнтські запити.

Одним з можливих вирішень завдань даного класу є концепція теорії математичних моделей прийняття оптимальних рішень в умовах конфлікту – рівновага Неша. Це така множина стратегій або дій у грі з двома чи більше гравцями, згідно з якими кожен учасник реалізує оптимальну стратегію, передбачаючи дії суперників, при якій жоден із учасників не може збільшити виграш, змінивши вибір стратегії в односторонньому порядку, коли інші учасники не змінюють свого вибору.

Разом з тим, це обумовлює доцільність удосконалення існуючих підходів балансування навантаження кластерних систем на основі рівноваги Неша, зокрема систем військового призначення, яке дозволить вирішити окреслену проблематику.

У зв'язку з цим, виникає актуальне наукове завдання пов'язане із розробкою адаптивного методу балансування навантаження кластерних систем військового призначення на основі рівноваги Неша.

Метою дослідження є підвищення ефективності існуючих механізмів балансування навантаження кластерних систем військового призначення.

Виклад основного матеріалу. Суть запропонованого методу, яка відрізняє його від існуючих, полягає, у першу чергу, в декомпозиції кожного завдання, як наслідку клієнтського запиту на симетричні підзадачі програмним засобом для розподілених паралельних обчислень MapReduce, а також у знаходженні рівноваги Неша на множині змішаних стратегій даних підзадач шляхом визначення для них імовірнісного розподілу паралельного використання серверів із врахуванням динаміки впливових на процес балансування навантаження чинників (рівень завантаженості серверів, складність задач) в умовах прийнятної обчислювальної складності. Так, поява нового завдання призведе до його декомпозиції на підзадачі з подальшим оптимальним розподілом їх паралельної обробки. Такий підхід дозволяє забезпечити ефективне використання серверних ресурсів у рівновазі за Нешем з максимальною конвергенцією до соціального оптимуму. Процес адаптивного балансування навантаження на основі рівноваги Неша представлено функціональною схемою, яка передбачає реалізацію наступних етапів (рисунок 1):

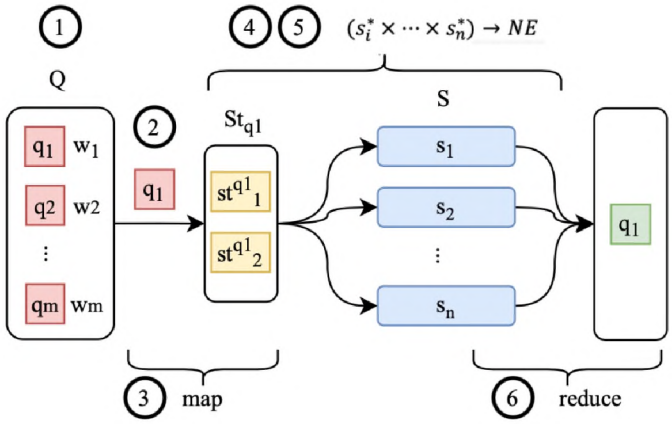


Рис. 1. Функціональна схема балансування навантаження кластерної системи на основі рівноваги Неша

1. Ініціалізація

На даному етапі визначаються завдання, суб'єкти, об'єкти, умови, а також виграші некооперативної гри процесу балансування навантаження.

Гра (G)*:* теоретико-ігровий варіант процесу динамічного балансування навантаження кластерної системи представлено як некооперативну гру у нормальній формі з ненульовою сумою на змішаних стратегіях (комбінація чистих стратегій із певною частотою), оскільки саме такий підхід дозволяє достатньо повно описати сервісну взаємодію кластера із клієнтами у процесі задоволення інформаційних потреб останніх $Q = \{q_1, \cdots, q_i, \cdots, q_m\}$, а також гарантує наявність хоча б однієї рівноваги за Нешем на будь якому профілі стратегій. Гравці SQ_{q_i} поділяють спільний набір стратегій $S = \{s_1, \cdots, s_i, \cdots, s_n\}$. Завдання – діяльність сервера, спричинена запитом користувача q_i із вагою w_{q_i}, що характеризує рівень його складності.

Гравці (SQ_{q_i})*:* у ролі гравців представлено підзадачі $SQ_{q_i} = \{sq_1^{q_i}, \cdots, sq_2^{q_i}\}$ отриманих завдань $q_i \in Q$ кластерною системою з відповідними вагами складності внаслідок запитів користувачів $Q = \{q_1, \cdots, q_i, \cdots, q_m\}$, що дозволяє уникнути неконтрольованої кількості гравців і стохастичної динаміки обчислювальної складності процесу балансування навантаження між серверами кластерної системи. Кількість підзадач дорівнює 2, оскільки на практиці доведено існування рівноваги за Нешем на змішаних стратегіях для біматричної гри (будь яка кількість стратегій для 2-х гравців).

Стратегії (S): існуюча множина усіх можливих стратегій (серверів кластерної системи) $S = \{s_1, \cdots, s_i, \cdots, s_n, C_{s_n}^k\}$, де $C_{s_n}^k$ – підмножина усіх можливих змішаних стратегій (комбінацій чистих стратегій s_i) без повторень, k – потужність множини підзадач SQ_{q_i}.

Виграші (U_i): Виграш, який отримує підзадача $sq_j^{q_i}$ залежить від отриманого профілю стратегій $s_i^* \times \cdots \times s_n^*$ внаслідок некооперативного вибору кожною підзадачею сервера $s_i \in S$. Кожна підзадача $sq_j^{q_i}$ намагається максимізувати свій виграш U_i шляхом мінімізації власного часу на обробку (обрати сервер з поміж наявних у кластерній системі із найменшим навантаженням l_{s_i}). Виграші – значення завантаженості серверів l_{s_i} за показником очікуваного часу обробки підзадач.

Результат: визначення стійкого у рівновазі та оптимального профілю використання серверних ресурсів кластерної системи під час обробки множини підзадач SQ_{q_i} із максимальним відсотковим значенням конвергенції (міри збіжності) знайденої рівноваги Неша до соціального оптимуму.

2. Отримання завдання

На даному етапі передбачається прийом множини зважених завдань балансувальником внаслідок отримання користувальницьких запитів $Q = \{q_1, \cdots, q_i, \cdots, q_m\}$.

3. Декомпозиція завдання на підзадачі

Отримане завдання q_i декомпозується балансувальником навантаження на множину підзадач $SQ_{q_i} = \{sq_1^{q_i}, \cdots, sq_2^{q_i}\}$, потужність якої дорівнює 2. Підхід до логічної декомпозиції задачі базується на програмній моделі MapReduce для розподіленої паралельної обробки великих масивів даних із використанням кластерів, який показує значну ефективність у галузях Big Data, розподіленого пошуку та сортування даних, звернення графа веб-посилань, обробки статистики логів мережі, побудови інвертованих індексів, кластеризації документів, машинного навчання та статистичного машинного перекладу. Використання даного підходу передбачає реалізацію процедури *map* – попередньої обробки завдання q_i та його ваги w_{q_j} як переліку значень балансувальником у вигляді списку, проте на відміну від класичної моделі MapReduce балансувальник навантаження ділить згенерований список на дві підзадачі та передає їх на етап обчислення виграшів U_i у платіжній матриці.

4. Обчислення виграшів

Кожна підзадача $sq_j^{q_i}$ намагається максимізувати свій виграш U_i (обрати сервер із найменшим навантаженням l_{s_i} з метою максимізації його ресурсів для мінімізації власного часу на обробку $t_{sq_j^{q_i}}$).

Розрахунок серверного навантаження l_{s_i} у платіжній матриці ґрунтується на основі відношення суми ваг w_{sq_j} усіх підзадач $sq_j^{q_i}$ різних завдань q_i, що ним обслуговуються із відповідною швидкістю v_{s_i}, яку регламентовано технічними характеристиками сервера s_i (1):

$$l_{s_i} = \sum_{1}^{n} \frac{w_{sq_j^{q_i}}}{v_{s_i}} + \xi \qquad (1)$$

де ξ – власне навантаження сервера, не викликане клієнтськими запитами.

Значення виграшів U_i у платіжній матриці розраховуються на основі показника l_{s_i} із врахуванням очікуваного часу на обробку $t_{sq_j^{q_i}}$ для кожної нової підзадачі $sq_j^{q_i}$ на множині серверів (2):

$$U_i\left(sq_j^{q_i}\right) = l_{s_i} + \frac{w_{sq_j^{q_i}}}{v_{s_i}} \qquad (2)$$

5. *Балансування навантаження*

NE (Nash equilibrium) – процедура пошуку рівноваги за Нешем на множині змішаного вибору серверів шляхом визначення такого імовірнісного розподілу для кожної підзадачі $sq_j^{q_i} \in SQ_{q_i}$, щоб значення їх виграшів на платіжній матриці були рівними на усіх стратегіях $s_i \in S$ (3, 4).

$$NE: p(sq_1^{q_i} \to S) = \begin{cases} p_{sq_1^{q_i}}(s_i) = p_{sq_2^{q_i}}(s_i) * u_{11} \pm \left(\sum_{s_i \epsilon S} p_i(s_i) - p_{sq_2^{q_i}}(s_i) \right) * u_{1n} \\ p_{sq_1^{q_i}}(s_n) = p_{sq_2^{q_i}}(s_i) * u_{n1} \pm \left(\sum_{s_i \epsilon S} p_i(s_i) - p_{sq_2^{q_i}}(s_i) \right) * u_{nn} \end{cases} \quad (3)$$

$$NE: p(sq_2^{q_i} \to S) = \begin{cases} p_{sq_2^{q_i}}(s_i) = p_{sq_1^{q_i}}(s_i) * u_{ii} \pm \left(\sum_{s_i \epsilon S} p_i(s_i) - p_{sq_1^{q_i}}(s_i) \right) * u_{ni} \\ p_{sq_2^{q_i}}(s_n) = p_{sq_1^{q_i}}(s_i) * u_{in} \pm \left(\sum_{s_i \epsilon S} p_i(s_i) - p_{sq_1^{q_i}}(s_i) \right) * u_{nn} \end{cases} \quad (4)$$

Таким чином, на основі отриманого імовірнісного розподілу $p(sq_j^{q_i})$ досягається оптимальний профіль серверів для кожної підзадачі $sq_j^{q_i}$ у відповідь на змішаний вибір серверів $s_i \in S$ іншою підзадачею $sq_j^{q_i}$, оскільки забезпечується рівність значень функції виграшу на різних серверах. Іншими словами, після процедури NE окремій підзадачі $sq_j^{q_i}$ без різниці, який із серверів буде обрано іншою підзадачею (у будь якому випадку виграш буде однаковий).

Варто зауважити, що пошук рівноваги за Нешем на змішаних стратегіях на основі (3, 4) у більшості випадків справедливий для гри, у платіжній матриці якої немає домінуючих (строго домінуючих) змішаних стратегій.

У випадку наявності в платіжній матриці домінуючих (строго домінуючих) змішаних стратегій (значення отриманого імовірнісного розподілу може виходити за межі $0 \leq sq_j^{q_i} \leq 1$) пошук точки рівноваги необхідно вирішувати на основі підходу вибору домінуючих (строго домінуючих) змішаних стратегій (виключення стратегій, що домінуються).

Вибір сервера s_i^* є строго домінуючим для окремої підзадачі $sq_j^{q_i}$ у грі балансування навантаження серверів кластерної системи, якщо він строго домінує будь-який вибір іншого сервера $s_i \in S$.

Кожна чиста стратегія гравця може розглядатися як його змішана стратегія, у якій дана чиста стратегія вибирається з ймовірністю 1, а решта – з ймовірністю 0. Так, визначення ситуації рівноваги ґрунтується на твердженні, що стратегія, яка строго домінується іншою не може входити у будь-яку рівновагу за Нешем (імовірність вибору даної стратегії у процесі змішування дорівнює нулю). До того ж, змішаний вибір серверів зможе бути таким, який строго домінується навіть у випадку якщо він використовує чисті стратегії із позитивною імовірністю, які не є такими, що домінуються.

У зв'язку з цим, у профілі змішаного вибору серверів завжди існує хоча б одна рівновага за Нешем. Узагальнена схема оптимального профілю серверів представлено на рисунку 2.

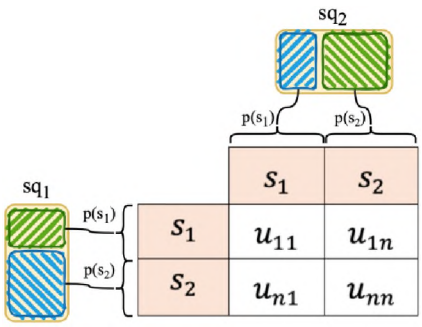


Рис. 2. Узагальнена схема профіля серверів на основі рівноваги за Нешем

Таким чином, на основі визначеної рівноваги за Нешем на профілі змішаного вибору серверів $s_i \in S$ підзадачами $sq_j^{q_i} \in SQ_{q_i}$ до кожного серверу s_i передається вказана частина підзадачі для подальшої обробки, розмір якої відповідає частоті його вибору у грі адаптивного балансування серверного навантаження кластерної системи, що призводить у свою чергу до отримання оптимального та водночас стійкого варіанту використання наявних серверних ресурсів.

Далі множина (пара) підзадач SQ_{q_i} розподіляється на профіль серверів $s_i \in S$ за вказівкою отриманого значення розподілу, де кожен сервер $s_i \in S$, який отримав підзадачу записує результат у форматі "ключ-значення" (ключі раніше створені процедурою *map*) у тимчасове сховище для подальшої обробки.

6. Об'єднання підзадач

На даному етапі процесу балансування навантаження кластерної системи на основі рівноваги за Нешем передбачається реалізація процедури *reduce* – паралельна розподілена обробка кожним сервером груп даних по порядку проходження ключів та з'єднання результатів балансувальником навантаження. Отриманий результат – є рішенням завдання, отриманого на основі користувальницького запиту $q_i \in Q$.

Висновки:

Таким чином, запропонований підхід дозволяє вирішити вищезазначену проблематику, а саме:

– пошук рівноваги у змішаних стратегіях завжди має рішення;

– кількість гравців обмежено біматричною грою, що дозволяє знаходити рівновагу за Нешем за досить короткий час;

– метод ефективно адаптується до динаміки значень усіх розглянутих впливових на процес балансування навантаження чинників;

– виведення з ладу одного із серверів не призводить до втрати завдань у цілому, які йому було делеговано, втрачається лише їх частина (можливо відновити за контрольною сумою).

Отримані результати відповідають актуальним вимогам до функціонування ІС критичної інфраструктури держави, зокрема ІС військового призначення у контексті їх стабільності (неперервності) та надійності).

Перспективним напрямком подальших наукових досліджень є розробка методу інтелектуального зважування задач балансувальником навантаження, отриманих внаслідок запитів користувачів шляхом застосування методів та систем штучного інтелекту, зокрема нейронних мереж.

Фесенко О.Д. (ВІТІ ім. Героїв Крут)

МЕТОДИКА КЕРУВАННЯ ТРАЄКТОРІЄЮ БПЛА В АВТОНОМНОМУ РЕЖИМІ ПОЛЬОТУ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО АЛГОРИТМУ MELM – MADGWICK.

Актуальність. На сьогодні одним із пріоритетних напрямків застосування безпілотних літальних апаратів (БПЛА) як у військових діях (розвідка, ударні дрони) так і цивільній сфері діяльності (дослідження складних рельєфів місцевостей, тощо). Як правило для вирішення вищезазначених завдань застосовується, швидкісні БПЛА мініатюрного типу які мають ряд переваг над габаритними БПЛА[1]:висока мобільність; дешевизна; застосування ресурсозберігаючих технологій; маскування; високе маневрування в просторі.

Функції керування маршрутом польоту без сигналів глобальних систем позиціювання (ГСП), в межах даного дослідження, виконують безплатформні інерціальні навігаційні системи (ІНС), побудовані на основі МЕМС-датчиків [2].

Із зростанням часу безперервної роботи збільшується помилка встановлення маршруту (далі-точність).

Одна із причин похибок оцінкиІНС – явище не стабільності нуля гіроскопа (BiasInstability), викликане шумом обробки інформації показників в електронних компонентах(флікер шумом англ. Flickernoise) [3].

По-друге, більшість МЕМС гіроскопів які застосовуються в навігаційних системах БПЛА мають похибку випадкового блукання кута – AngleRandomWalk на рівні 0,02-0,06 °/с.

Крім того, температурні варіації елементної бази призводять до статичного приросту похибок коефіцієнтів перетворенняі складають 0,5-3% [3].

Відомо, що інерціальні навігаційні системи на базі МЕМС – датчиків, мають високу чутливість, що призводить до виникнення похибок оцінки встановлення кутової швидкості, визначення курсу, яка становить $\Delta_{\omega} \in \{0.66 \dots 1.16\}^{\circ}/\text{с}$. [4,5], відповідно без корегування GPS навігації, похибки МЕМС інерціальної навігаційної системи збільшуються із часом.

Постановка задачі.В результаті раптового зникнення сигналів ГСП, інерціальна навігаційна система починає працювати у автономному режимі – тільки на основі показників МЕМС – датчиків (акселерометр, гіроскоп,магнітометр)[6], та відомо, що структура моделі похибок МЕМС – датчиків БІНС, через нестабільністьність окремих складових, особливо в період кореляції, близький до періоду зникнення сигналу ГСП (від 10 до 300 с),може стати критичною для виконання всієї місії польоту БПЛА [4-6].

Крім того, під час маневрування БПЛА в динамічному середовищі в автономному режимі польоту донавігаційної системи МЕМС на базі нейромережевих алгоритмів пред'являються вимоги:

– похибка відхилення від цільової траєкторії $T(\Delta_{\omega БПЛА}) \leq \{0.012 \dots 0.18\}^{\circ}/\text{с}$ [6,8,9];

–період навчання нейромережі $t_{lerningperiod} \leq \{20 \dots 100\}$с., обумовлено обмеженням фізичним сховищем пам'яті мікроконтролера на базіArduinota встановленням необхідного довірчого інтервалу репрезентативності навчальної вибірки еталонних навігаційних параметрів[7,8];

Не виконання вище зазначених вимог може призвести до відхилення від цільової траєкторії до 400 метрів на 1 кілометр польоту, що показано в роботі.

Таким чином метою доповіді пропонується розглянути методику керування траєкторією БПЛА в автономному режимі польоту, суть якої полягає в зменшенні відхилення від цільової траєкторії БПЛА в умовах раптового зникнення сигналів GPS (на час від 10 до 300 с), шляхом застосування вдосконаленого фільтра Маджвіка та нейронної мережі на основі алгоритму MELM.

Основні положення.На сьогодні, задача підвищення точності позиціювання БПЛА у під час відсутності сигналів глобальної системи навігації вирішується як правило за допомогою варіацій алгоритмів фільтрацій Калмана в синтезі із застосуванням алгоритмів машинного навчання та нейронних мереж. Однак виникає низка протиріч розробки інтелектуальних систем навігації для мікро та малих класу БПЛА:

1. Обмеження обчислювальної складності мікрокомп'ютерногообладнання БПЛА;
2. Часова затрата навчання нейронної мережі в динамічному середовищі;
3. Квантування навчаної нейронної мережі.

Одним із вирішенням вищезазначених задач є алгоритми автоматичного пошуку моделі нейромережевих структур, що дозволяє максимально точно підібрати модель нейромережі для вирішення цільової задачі враховуючи обмеження.

Аналіз останніх публікацій.Один із відомих методів автоматизованого машинного навчання єалгоритмагностичної мережі підбору нейронної архітектури WANN [9], на відміну від традиційних алгоритмів WANN замість під лаштування вагових коефіцієнтів, використовує варіаційний процес на основі генетичного методу підбору архітектури нейромереж з загальним ваговим коефіцієнтом, що скорочує час на адаптацію вибраної архітектури нейронної мережі для вирішення цільової задачі.

В роботі [9] алгоритм WANN вперше був застосований для вирішення задач автономної навігації БПЛА, а саме процесу компенсацій похибок гіроскопу кутового прискорення інерціальної навігаційної системи МЕМС. Експериментальний аналіз трьох алгоритмів штучних нейронних мереж пошуку нейронної архітектури Neural Architecture Search recurrent neural network (NAS-RNN), коротко та довготривалої рекурентної мережі Long short-term memory recurrent neural network (LSTM-RNN) та агностичної мережі підбору архітектури Weight Agnostic Neural Networks (WANN) показали, що при застосуванні NAS-RNN значення стандартного відхилення тривісних вимірювань гіроскопу зменшилися відповідно на 44,0%, 34,1% та 39,3%. В свою чергу архітектура WANN-RNN не залежить від окремо взятого вагового коефіцієнта. При цьому в якості додаткової цілі для оптимізації мінімізують кількість нейронів мережі. Крім того, архітектура WANN-RNN за результатом експерименту забезпечує найкращий результат по рівню похибки встановлення параметрів гіроскопу та істотно зменшилась у 7,2; 0,92; 0,87 разів відносно NAS-RNN.

Однак, для реалізації в реальному часі вище зазначених нейромережевих алгоритмів на базі технології МЕМС малогабаритних мікрокомп'ютерів Arduino, як правило, потребують процесу квантування нейромережі [10] (для зниження розмірностіархітектури нейромережі), але точність таких нейромереж знижується на 20 – 30%.

На сьогодні для розробки інтелектуальних систем навігації переважно застосовують динамічні нейронні мережі [11], які дозволяють уникнути процесу квантування без втрати точності нейромережевоїмоделі. Тому, пропонується розглянути альтернативні алгоритми на основі екстремального машинного навчання (Extreme learning machine – ELM), які були представлені Хуангом Г.Б. [12]. Відмінність алгоритму машинного навчання ELM від традиційних алгоритмів полягає в швидкості навчання, абсолютно не використовує ітераційних алгоритмів оптимізації (варіація алгоритмів градієнтного спуску) для мінімізації помилки цільової функції.

На сьогодні вчені представили багато варіацій алгоритму нейронної мережі на базі ELM. Один із таких варіацій є динамічна модифікована багаторівнева структура алгоритму MELM [13] (*multihidden-layer ELM*), яка може застосовуватись в системах МЕМС технології. На відміну від традиційних нейромережевих алгоритмів, MELM в процесі навчання не залежить від репрезентативності вихідних даних, динамічно підлаштовується (процес адаптивного підлаштування архітектури нейромережі) під обчислювальні вимоги в процесі навчання.

Виклад основного матеріалу. В момент раптового зникнення сигналу глобальної системи позиціювання для визначення оцінки позиціювання безпілотного літального апарату, тобто (швидкість і положення БПЛА), застосовується алгоритм вдосконаленої фільтрації Маджвіка (обробки даних GPS і МЕМС ІНС), які одночасно надходять в блок нейронної мережі (див. рис. 1) та відбувається процес навчання в реальному часі, далі навчена модель нейронної мережі на основі алгоритму MELM використовується в якості заміни сигналу GPS для прогнозування позиції БПЛА в просторі

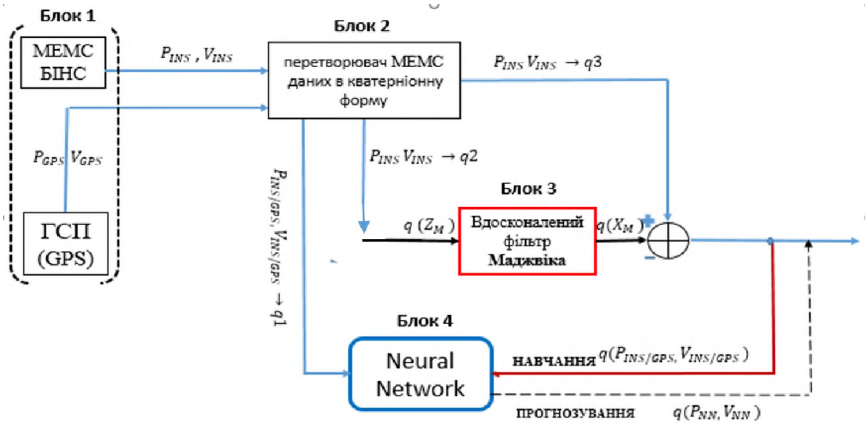


Рисунок 1 – Блок схема реалізації методики управління траєкторією БПЛА

Методика управління траєкторієюБПЛА в автономному режимі польоту складається з 4-ох етапів:

На першому етапі блок 1 (див. рис 1)відбувається обробка даних мікро - електромеханічної системи (МЕМС) безплатформної інерціальної навігаційної системи (БІНС)та глобальної системи позиціювання (ГСП) типу GPS для визначення параметрів еталонної траєкторії БПЛА;

Модель траєкторії БПЛА будується на основі данихнавігаційної системи глобальної системи позиціювання GPS та процесів роботи МЕМС інерціальної системи навігації вдосконаленого фільтру Маджвіка, яка в сутності представляє собою 18-мірний вектор стану, що показано в рівнянні (1):

$$P = \left[\phi_{E,N,U}\ \Delta V_{E,N,U}\ \Delta P_{l,\lambda,h}\ \Delta g_{x,y,z}\ \Delta a_{x,y,z}\ \Delta m_{x,y,z}\right]^T, \quad (1)$$

де $\phi_{E,N,U}$ – вектор похибки орієнтації відносно платформи БПЛА, який представляє собою проекцію обертання Землі на осі (east-north-up), $\Delta V_{E,N,U}$ – похибки даних швидкості БПЛА відносно локальної системи координат БПЛА, $\delta_{l,\lambda,h}$ – похибка довготи, широти та висоти, $\Delta g_{x,y,z}$ – похибки постійного відхилення гіроскопа в системі координат відносно МЕМС датчиків, $\Delta a_{x,y,z}$ – похибки постійного зміщення акселерометра, $\Delta m^E{}_{x,y,z}$ – похибки магнітометра (феромагнітний вплив) відносно визначення магнітної півночі, індекс E – еталонна модель магнітного поля.

На другому етапі блок 2 (див.рис. 2)відбувається процес перетворення МЕМС даних в кватерніону форму.

Функція блоку перетворювача МЕМС даних полягає в поєднанні навігаційних даних в єдину кватерніонну форму, що сприяє мінімізації часу обробки навігаційних даних за рахунок властивостей кватерніона, а саме зменшення розмірності вхідних навігаційних параметрів, тобто 18-ти мірний вектор стану перетворюється в 6-ти мірний, як показано в рівнянні (3), також

перевага застосування кватерніона за умови обмеження фізичних параметрів флеш пам'яті ≤ 2000 kb на базі мікроконтролерів Arduino.

$$f(\phi_{E,N,U}\Delta V_{E,N,U}\Delta P_{l,\lambda,h}) \rightarrow q(q1(\phi_{E,N,U}), q2(\Delta V_{E,N,U}), q3(\Delta P_{l,\lambda,h}) \quad (2)$$

На третьому етапі блок 3 (див. рис. 2),відбувається процес роботи вдосконаленого алгоритму фільтрації Маджвіка[13].

На третьому етапі блок 4. Алгоритм навчання нейронної мережі на основі MELM.

Для мінімізації впливу вище зазначених обмежень, було застосовано багаторівневу архітектуру (Multihidden – layer – Extreme Learning Machine)MELM, що зменшує обчислювальну складність без обмеження фізичної пам'яті навігаційної системи БПЛА МЕМС на базі Arduino та відповідно для зменшення відхилення від цільової траєкторії БПЛА після моменту втрати сигналів GPS.

На рисунку 3 показано Блок схема роботи алгоритму MELM з вхідними і вихідними параметрами навігаційних даних в кватерніонній формі.

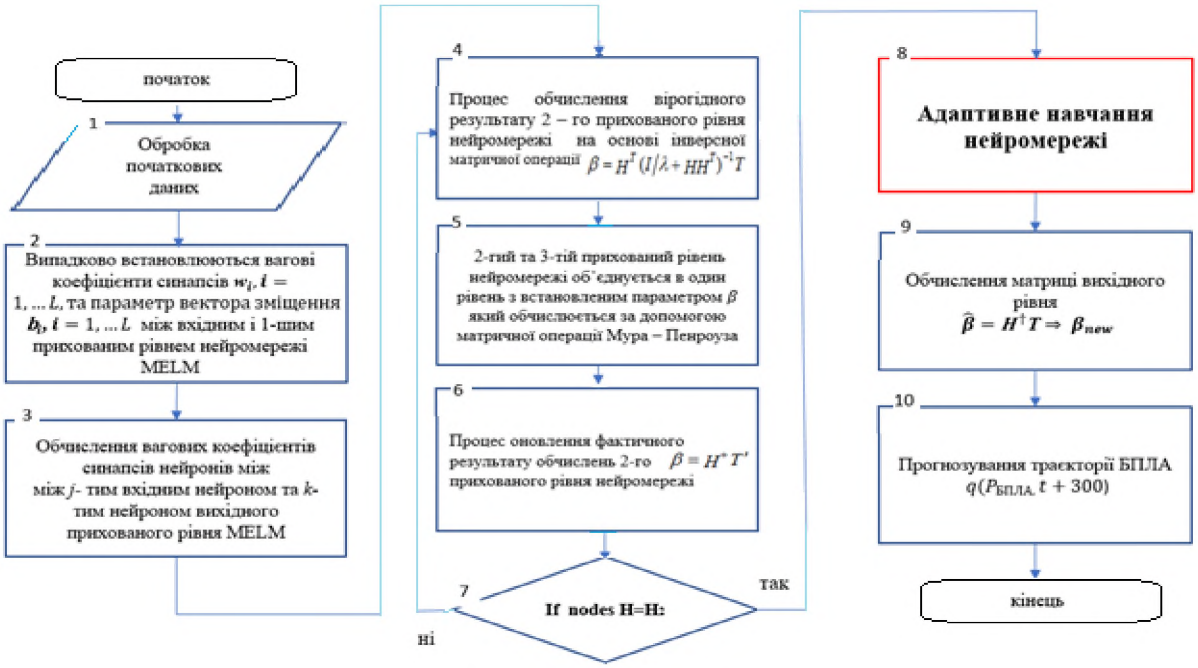


Рисунок 2 – Роботи алгоритму MELM з вхідними і вихідними параметрами

Для перевірки працездатності запропонованих методики керування траєкторією бпла в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick були проведені триекспериментальних дослідження на програмно апаратній інтеграцій.

Для визначення ефективності запропонованої методики, а саме, процесу прогнозування оцінки позиціювання безпілотного літального апарату (швидкість і положення БПЛА), порівнюється алгоритм вдосконаленого фільтра Маджвіка на основі нейромережі MELM (MELM – Madgwick), з алгоритмом ELM – Kalman та WANN – RNN Madgwick .

Вхідні дані: $Q=\{q1(\phi_{E,N,U}), q2(\varepsilon V_{E,N,U}), q3(\varepsilon P_{l,\lambda,h})\}$ – вектор еталонних параметрів позиціювання БПЛА.

Вихідні дані: $T=\{q1(\phi_{E,N,U}+\Delta_{t-1}), q2(V_{E,N,U}+\Delta_{t-1}), q3(P_{l,\lambda,h}+\Delta_{t-1})\}$ – цільові вихідні параметри прогнозування траєкторіїБПЛА в автономному режимі польотупід час зникнення сигналу GPS.

Обмеження: $T(\Delta_{\omega БПЛА}) \leq \{0.012 \dots 0.18\}^{\circ}\frac{1}{c}$ – ідхилення від цільової траєкторії БПЛА в автономному режимі польоту [4-6]

період навчання нейромережі - $t_{lerning\ period} \leq \{10 \dots 100\}$с.

швидкість адаптивного навчання нейромережі (процес до навчання нейромережі в період появи сигналів GPS) – $t_{adaptive\ retraining\ period} \leq \{0.034 \dots 0.05\}$с.

Цільова функція: $F(T(\Delta_{\omega БПЛА})) \rightarrow min \Rightarrow \min_{\beta} \|H\beta - T^{`}\| \Rightarrow optimum(NNA)$.

Допущення: Швидкість польоту БПЛА є сталою, і складає 40 км/год.

Експеримент 1. Мета експерименту - визначення впливу кількості нейронів прихованого рівня нейронної мережі на швидкість їх навчання на точність апроксимації навігаційних даних. В цьому випадку використовуються адаптивні властивості нейромережі MELM, зокрема, здатність нейромережі апроксимувати, а потім екстраполювати вхідні сигнали досить складної форми. При цьому, задаючи структуру нейромережі, можна варіювати складність нейромережевої структури. На вхід нейромережі подається навчальна вибірка, вектор параметрів похибки позиціювання та еталонної моделі позиціювання БПЛА, а на виході отримуємо параметри прогнозування позиції і швидкості БПЛА.

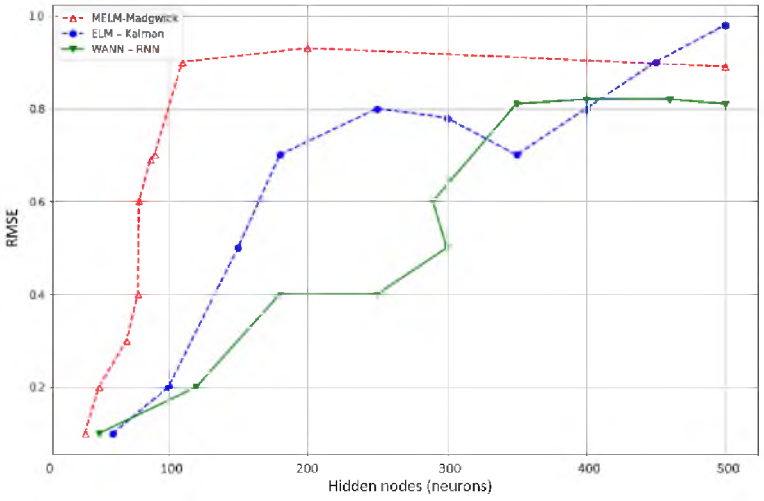


Рисунок 3 – Графік оцінки точності навігаційних параметрів БІНС на основі нейромережевих алгоритмів із різною кількістю нейронів прихованого рівня

Структура мережі може включати кількість вхідних нейронів, що перевищує число вимірюваних сигналів, тому застосовуються властивості нейромережі MELM, а саме в постійному процесі підналаштованні параметрів таким чином, щоб мінімізувати різницю вихідних даних МЕМС ІНС (позиціювання і швидкості) і даних позиціювання і швидкості отриманих з використанням сигналів GPS.

На графіку (рис. 3) порівнюється результат роботи трьох алгоритмів БІНС, використовується популярна метрика похибок root mean square error (RMSE) для вимірювання різниці між значеннями прогнозування моделі і еталонної моделі. А саме, було здійснено оцінку точності визначення навігаційних параметрів БІНС на основі нейромережевих алгоритмів. Таким чином, результат імітації параметрів сигналу GPS:

MELM-Madgwick позначений на графіку червоною лінією, із результатом 100 нейронів прихованого рівня – точність у відсотковому співвідношенні RMSE складає 88.4%);

ELM – Kalman блакитною лінією (результат 500 нейронів – точність у відсотковому співвідношенні RMSE складає 93.2%);

WANN –RNN Madgwick зеленою лінією (результат 500 нейронів - точність у відсотковому співвідношенні RMSE складає 81.3%).

Експеримент 2. Мета експерименту – визначення швидкості процесу адаптивного навчання нейромережевих алгоритмів БІНС БПЛА.

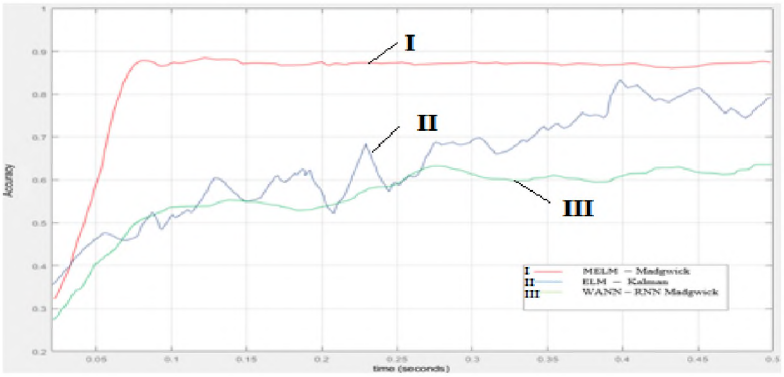


Рисунок 4 – Графік точності і часу адаптивного навчання БІНС в залежності від типу нейромережевого алгоритму.

Експеримент полягав в тому, що при тестуванні навченої нейромережі на її вхід подавалися тестові вектори, відмінні від використаних в навчальній послідовності.

В результаті експерименту встановлено:БІНС на основі нейронної мережі MELM-U-Madgwick (I) (швидкість навчання – 0.06 с, точність у відсотковому співвідношенніRMSE – 93.2%);

БІНС на основі нейронної мережі ELM – Kalman (II) (швидкість навчання склала 0.8 с, точність у відсотковому співвідношенніRMSE - 80.2%) в процесі адаптації також видно на графіку вплив нових даних яких нейромережа небачила сутєво впливають на збіжність нейромережі;

БІНС на основі неромережевого алгоритму WANN –RNN Madgwick (III) (швидкість навчання 0.81 с ,точність у відсотковому співвідношенніRMSE -65,4%).

Експеримент 3. Мета експерименту - дослідження якості БІНС на основі досліджуваних алгоритмів нейронної мережі за прогнозуванням впливу відхилень параметрів орієнтації та навігації при використанні нейромереж замість GPS. На рисунку 6 – 8 показано результат прогнозування параметрів траєкторії БПЛА.

В таблицях 1 – 3 показано результат прогнозування параметрів траєкторії БПЛА.

Таблиця 1

Географічні дані побудови траєкторії БПЛА	Похибка прогнозування позиції БПЛА
Latitude(широта)	≈30.34 (м)
Longitude(довгота)	≈33.45 (м)
Altitude(висота)	≈32.12 (м)

Таблиця 2

Географічні дані побудови траєкторії БПЛА	Похибка прогнозування позиції БПЛА
Latitude(широта)	≈100.12 (м)
Longitude(довгота)	≈118.95 (м)
Altitude(висота)	≈120.13 (м)

Таблиця 3

Географічні дані побудови траєкторії БПЛА	Похибка прогнозування позиції БПЛА
Latitude(широта)	≈90.11 (м)
Longitude(довгота)	≈92.55 (м)
Altitude(висота)	≈95.12 (м)

Таблиця 1 – Робота алгоритму MELM–Madgwick в процесі прогнозування географічних параметрів БПЛА (на 300 с польоту БПЛА без урахування ГСП похибка позиціювання відносно еталонних географічних параметрів (таблиця 1), становила ≈30–33 м і збільшувалася із часом).

Таблиця 2 – Робота алгоритму WANN– RNN–Madgwick в процесі прогнозування географічних параметрів БПЛА (на 300 с польоту БПЛА без урахування ГСП похибка позиціювання відносно еталонних географічних параметрів (таблиця 2), становила ≈100–120 м і збільшувалася із часом).

Таблиця 3 – Робота алгоритму ELM – Kalman в процесі прогнозування географічних параметрів БПЛА (на 300 с польоту БПЛА без урахування ГСП похибка позиціювання відносно еталонних географічних параметрів (таблиця 3), становила ≈90–95 м і збільшувалася із часом).

Результат експериментівна часовому інтервалі t = 100 с, на основі GPS даних та на інтервалі їх відсутності (t = 300 с польоту БПЛА) показав, що застосування алгоритму на основі ELM – Kalman точність навчання нейромережі БІНС була кращою в порівнянні з алгоритмом MELM – Madgwick на 13.94% та WANN–RNN–Madgwick на 29.82%. Однак необхідно зазначити, що точність навчання покращувалась із зростанням кількості нейронів в структурі прихованого рівня < 500, що підвищує обчислювальну складність та відповідно збільшує час навчання нейромережі. Тому реалізація такого алгоритму на комп'ютерному обладнані мікро – БПЛА не задовольняє вище зазначеним вимогам.

В свою чергу застосування розробленої методики керування траєкторією БПЛА в автономномному режимі польоту на основі нерйромережевого алгоритму MELM–Madgwick дозволило здійснити адаптацію структури прихованого рівня, яка стаовить 100 нейронів прихованого рівня рис , що дозволяє використання алгоритму MELM–Madgwick у якості компромісного варіанту.

Крім того, завдяки проведеному імітаційному моделюванню, результат дослідження застосування запропонованих нейромережевих алгоритмів для заміни вхідних даних замість сигналів GPS на вхід БІНС, дозволив оцінити похибку позиціювання відносно еталонної моделі на основі сигналів GPS.

Сутність методики, що визначає її новизну та відмінність від відомих методів, полягає:

по-перше, інтегрувати розроблений алгоритм в системи управління БПЛА на базі МЕМС технології мікрокомп'ютерівArduino Nano, під час зникнення GPS сигналу, на часовому інтервалі t = (10...300 с), що являється критичним для класу мікро та малих безпілотників;

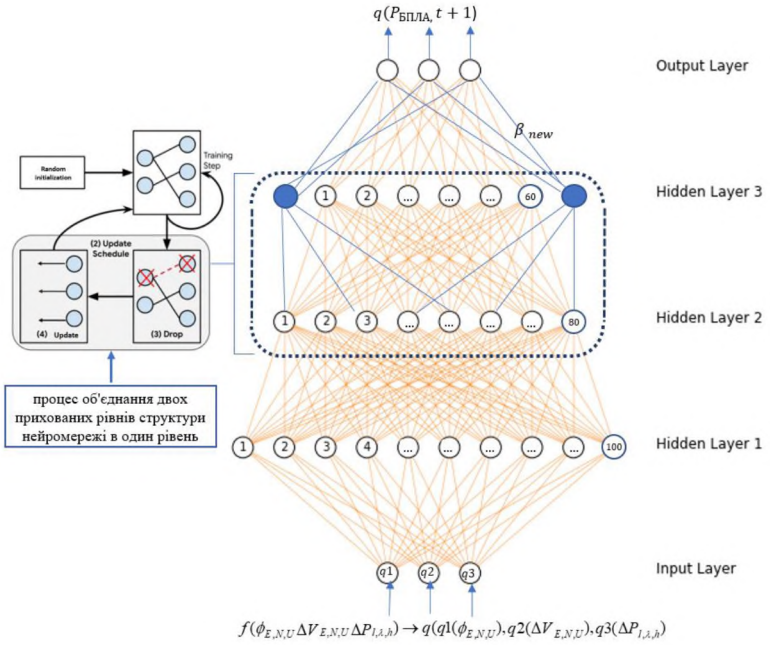


Рисунок 5 –Процес оптимізації структури нейромережі MELM.

по-друге, розроблений алгоритм MELM–Madgwick дозволяє апроксимувати, та екстраполювати вхідні сигнали навігаційних параметрів в динамічному середовищі, при цьому відбувається процес адаптивного навчання в реальному часі (оптимізації нейромережевої структури) в залежності від зростаючої складності обчислення параметрів нейромережі, а саме збільшення кількості нейронів на прихованому рівні. Таким чином, запропонований алгоритм дозволяє змінювати структуру нейромережі адаптивним способом замінюючи приховані нейрони новоствореними прихованими вузлами з кращою продуктивністю, з урахуванням умови найменшої кількості нейронів прихованого рівня, а також найменшої помилки враховуючи обмеження;

по-третє, вперше було запропоновано застосувати блок перетворювача навігаційних даних в кватерніону форму для зменшення розмірності вхідних даних, що в свою чергу дозволило підвищити швидкість та точність навчання нейромережі без застосування процесу квантування;

по-четверте, вперше був застосований нейромережевий алгоритм MELM для вирішення задач автономної навігації для зменшення відхилення БПЛА від цільової траєкторії під час зникнення GPS сигналів;

в результаті застосування методики керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM–Madgwick під час зникнення глобальних супутникових систем позиціювання, похибка прогнозування навігаційних параметрів траєкторії найменша і склала ≈30–33 м, що додатково підтверджує доцільність його

Напрямком подальших досліджень є розробка інтелектуальної системи управління групою БПЛА з урахуванням особливостей організації каналів управління і зв'язку.

СПИСОКВИКОРИСТАНИХДЖЕРЕЛ.

1. Fendy Santoso, Matt Garratt, S.G. Anavatti, «State-of-the-Art Intelligent Flight Control Systems in Unmanned Aerial Vehicles» February 2017, IEEE Transactions on Automation Science and Engineering PP(99):1-15.

2. Yimin Zhou ; Jiao Wan ; Zhifei Li ; Zhibin Song "GPS/INS integrated navigation with BP neural network and Kalman filter" 2017 IEEE International Conference on Robotics and Biomimetics (ROBIO), **Date Added to IEEE Xplore:** 26 March 2018.

3. C. Sun, W. He, W. Ge, and C. Chang, "Adaptive Neural Network Control of Biped Robots," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 47, no. 2, pp. 315–326, 2017.

4. S. Ding, G. Ma, and Z. Shi, "A Rough RBF Neural Network Based on Weighted Regularized Extreme Learning Machine," Neural Processing Letters, vol. 40, no. 3, pp. 245–260, 2014.View at: Publisher Site | Google Scholar.

5. Fakharian, T. Gustafsson, M. Mehrfam, "Adaptive kalman filtering based navigation: an IMU/GPS integration approach" IEEE conference on networking, sensing and control 2011, pp. 181-185

6. Adam Gaier, David Ha, «Weight Agnostic Neural Networks» *[Submitted on 11 Jun 2019 (v1), last revised 5 Sep 2019 (this version, v2)].*

7. Фесенко О. Д. Експериментальний аналіз застосування нейронних мереж для керування траєкторією польоту БПЛА / О. Д. Фесенко, Р. О. Бєляков, Г.Д. Радзівілов, В.С. Гулій // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2020. - Вип. 1. - С. 97-112.

8. C. Jiang, S. Chen, Y. Chen. A MEMS IMU de-noising method using long short term memory recurrent neural networks LSTM-RNN sensors, vol. 18, no. 10, p. 3470, 2018.

9. Fesenko O., Bieliakov R., Radzivilov H. and oth. (2022) Method of improving the accuracy of navigation MEMS data processing of UAV inertial navigation system. National University «Zaporizhzhia Polytechnic». Radio Electronics, Computer Science, Control.The scientific journal. Published four times per year No 3(62) 2022.

10.Prediction of SINS/GPS Navigation Information by ELM Algorithm during GPS outages Yang Cao, Fangxiu Jiaa , Xun Jiang, Qing Zhang School of Mechanical and Engineering Nanjing University of Science and Technology Nanjing, China.

11.A Multiple Hidden Layers Extreme Learning Machine Method and Its Application Research Article | Open Access Volume 2017 |Article ID 4670187 | https://doi.org/10.1155/2017/4670187.

12.R. O. Bieliakov, H. D. Radzivilov, O. D. Fesenko, "Method of the intelligent system construction of automatic control of unmanned aircraft apparatus", Radio Electronics, Computer Science, Control. National University "Zaporizhzhia Polytechnic", Vocabulary. Part 28. Artificial intelligence vol. 1, 2019, pp. 218–229.

13.Fesenko O., Bieliakov R., Radzivilov H. and oth. (2020) Trajectory Control Method Of UAV In Autonomous Flight Mode Using Neural Network MELM Algorithm. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). 25-27 Nov. 2020. https://doi.org/10.1109/ATIT50783.2020.9349317.

Шемендюк О.В. (ВІТІ ім. Героїв Крут)
Нещерет І.Г. (ВІТІ ім. Героїв Крут)
Процюк Ю.О. (ВІТІ ім. Героїв Крут)

ТЕНДЕНЦІЇ ТА ОСОБЛИВОСТІ СТВОРЕННЯ СУЧАСНИХ ВІЙСЬКОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ: ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА

У сучасному світі спостерігається тенденція до збільшення обсягу інформації. Ця інформація має важливе значення для осіб, підприємств, організацій або держав, які її зберігають, обробляють та передають за допомогою інформаційно-комунікаційних систем (далі – ІКС).

Широке використання комп'ютерних технологій в системах автоматизованої обробки даних загострило проблеми захисту інформації, що циркулює в ІКС. Захист інформації в ІКС має ряд специфічних особливостей, пов'язаних з тим, що інформація, не суворо пов'язана з носієм, може легко і швидко копіюватися і передаватися каналами зв'язку. Тому при формування вимог до захисту інформації обов'язково повинні бути враховані всі особливості функціонування ІКС.

Забезпечення надійного захисту інформації в ІКС включає:

- забезпечення безпеки інформації в ІКС;
- систематичний контроль за безпекою;
- виявлення слабких сторін у системі захисту;
- обґрунтування та реалізація найбільш ефективних шляхів удосконалення та розвитку системи захисту;
- належне навчання користувачів.

Ключовими елементами ефективної системи безпеки є:

- моніторинг та контроль доступу до інформації;
- безпечне передавання даних;
- безпечне зберігання та видалення даних.

Для ІКС питання захисту інформації, що зберігається, обробляється чи передається каналами зв'язку, вирішується шляхом створення комплексної системи захисту інформації в ній, що передбачає здійснення комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІКС згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері технічного захисту інформації.

Нормативним документом, що визначає основи організації та порядок виконання робіт із захисту інформації в ІКС – порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІКС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу є НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі".

Особливої важливості та актуальності питання захисту інформації має у військових інформаційно-комунікаційних системах (далі – ВІКС), що функціонують в Збройних Силах України та тих ВІКС, що перебувають на етапі створення.

В практичній діяльності дуже часто стикаємось з ситуацією, коли Замовник хоче створити КСЗІ в ІКС, піднімає питання захисту інформації не розуміючи того, що КСЗІ в ІКС не є самоціллю. А саме, Замовник часто оперує складністю вимогдо КСЗІ, тоді як основним є формування вимог до функціональності системи (характеристик інформації, сервісів та користувачів).Звідси, уже формуються вимоги до захисту інформації, саме її властивості будуть впливати на те, як КСЗІ буде побудована в конкретній ІКС, які заходи та засоби, які реалізують способи, методи, механізми захисту інформації ввійдуть до складу КСЗІ.

Серед решти проблемних питань варто відзначити те, що документи на розробку конкретної ВІКС та КСЗІ в ній (Технічні завдання) відпрацьовуються без залучення Споживача ІКС (з ним ТЗ погоджується) та Виконавця робіт, що значно ускладнює подальший процес розробки і зводить докладені зусилля нанівець.

У сучасному світі ІТ-технологій з кожним днем набирає популярності використання хмарних сервісів. Хмарні технології все частіше починають використовуватися для різних цілей та потреб, до того ж їх використовують як звичайні поодинокі користувачі так і цілі організації та державні структури, школи, університети. Все більше організацій переводять свої потужності та сервіси у хмару. Безумовно використання хмарних сервісів несе велику кількість переваг, таких як: економія на апаратних ресурсах, зниження витрат та відповідальності за адміністрування систем, підвищення доступності, тощо.

Для виконання хмарних обчислень використовують центри обробки даних (далі – ЦОД), що являють собою сукупність серверів, які розміщені в одній мережі. Метою створення ЦОД є підвищення ефективності та захищеності. Для забезпечення достатнього рівня захисту центрів обробки даних використовується мережевий та фізичний фільтри та системи моніторингу активності в мережі. Крім того, важливо забезпечити відмовостійкість і надійне електроживлення ЦОДу.

Але з перенесенням систем у хмару виникають і нові завдання по контролю та захисту таких систем. Однією з таких проблем є захист інформації при її зберіганні, передачі та обробці у хмарі.

На сьогодні ринок насичений різними рішеннями щодо захисту серверів і ЦОД від різноманітних загроз а також атак. Проте, кількість цих завдань значно збільшилась внаслідок поступової заміни апаратних систем, що вважались класичними, на віртуальні платформи.

У зв'язку з цим, до вже відомих типів загроз додалися складності, пов'язані з контролем хмарного середовища, трафіку між гостьовими машинами та розмежуванням прав доступу. З'явились більш суворі вимоги зовнішніх регуляторів, а також розширилися внутрішні питання щодо політики захисту ЦОД. Станом на сьогодні, до роботи ЦОД висуваються суворі вимоги щодо закриття технічних питань та питань, пов'язаних з їх безпекою.

Головною причиною масштабного перенесення більшості систем на хмарні сервіси стала віртуалізація. Звісно ж, разом з цим, постає ряд завдань щодо забезпечення безпеки в новому середовищі. Це вимагає особливого підходу. Більшість загроз вже достатньо вивчені та для них розроблені заходи протидії. Однак, слід провести адаптацію цих заходів для використання в хмарному середовищі.

Одною з перших проблем з безпеки, яка виникає –це контроль та управління хмарними сервісами. Адже відслідкувати всі ресурси сервісів, віртуальних машин, процесів це досить важка справа. Даний тип загроз є високорівневим, так як він пов'язаний з керуванням безпосередньо хмарним середовищем, як єдиною ІКС, отже для нього необхідно налагоджувати індивідуальну систему захисту.

Для цього використовують модель управління ризиками для хмарних інфраструктур. За основу забезпечення фізичної безпеки взятий суворий контроль фізичного доступу до всіх елементів даної інфраструктури. Основою мережевого захисту є міжмережевий екран та захист від вторгнень. Під використанням міжмережевого екрану розуміють роботу з фільтрації, метою якої є розмежування внутрішніх мереж ЦОД на підмережі з різним рівнем довіри.

До наявних атак на хмарне середовище відносять наступні:

- традиційні атаки на програмне забезпечення;
- функціональні атаки на елементи хмарної інфраструктури;
- атаки, що спрямовані на клієнта хмарного середовища;
- атаки на контролер середовища (гіпервізор);
- атаки на системи керування.

Ефективна архітектура безпеки хмарного середовища має визначати та боротись з цими атаками.

Вирішенням проблем безпеки стають такі рішення:

- шифрування даних, що зберігаються;
- захист даних при передачі;
- аутентифікація користувачів;
- ізоляція користувачів один від одного.

Хмарні технології –це дуже перспективний напрямок, що постійно розвивається та позитивно впливає на майбутнє вдосконалення інформаційних технологій. Його необхідно впроваджувати в Збройних Силах України при побудові ВІКС. Питання безпеки та побудови

КСЗІ в цьому середовищі для ВІКС буде залишатись завжди актуальним, оскільки обробка інформації в ІКС без КСЗІ в ній – заборонена.

17 лютого 2022 року був прийнятий Закон України "Про хмарні послуги", який набрав чинності 16 вересня 2022 року. Цей закон визначив правові відносини, що виникають при наданні хмарних послуг, та встановлює особливості використання хмарних послуг серед інших військовими формуваннями. Згідно цього Закону, Кабінету Міністрів України поставлено завдання у шестимісячний строк після набрання ним чинності, привести у відповідність ряд нормативно-правових актів та інших розпорядчих документів, щодо надання та використання хмарних послуг.

Позитивний досвід побудови КСЗІ в хмарних системах має компанія GigaCloud, яка ще у 2018 році отримала атестат відповідності КСЗІ на власні майданчики GigaCenter та BeMobile, що дало оператору можливість будувати розподілені, повноцінні та відмовостійкі хмарні рішення, рівень безпеки яких відповідає вимогам державного регулятора щодо захисту інформації.

Тепер, щодо кібербезпеки ІКС.На даний час питання забезпечення кібербезпеки поки що розглядаються окремо для різних систем. Відповідно до чинного законодавства України серед пріоритетів державної політики у сфері кібербезпеки є формування умов для забезпечення кіберзахисту інформаційної інфраструктури України, передусім – об'єктів критичної інформаційної інфраструктури держави.

Таким чином, підвищення якості кібербезпеки у ВІКС повинне носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки – постійно вдосконалюватися.

Ефективність заходів у цій сфері повинна досягатися завдяки здійсненню оперативної оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики в кіберпросторі, а також їх завчасно ліквідовувати, і хоча ІКС існує в межах правового поля (інформаційного законодавства), проте першоосновою протидії кібератакам є технічна сторона питання. Рівні технічного захисту (фільтри) законодавчо не завжди встановлюються шляхом введення спеціальних (національних та міжнародних) стандартів, проте в цілому простежується взаємодія ВІКС та інформаційного законодавства.

Під об'єктом критичної інформаційної інфраструктури, до складу якої входить ВІКС, розуміється інформаційно - комунікаційна або технологічна система об'єкта критичної інфраструктури, виведення з ладу або руйнування якої безпосередньо вплине на національну безпеку і оборону України,.

Постановою Кабінету Міністрів України 19 червня 2019 року № 518 "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" були затверджені Загальні вимоги. Ці вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури. Також в цих вимогах визначено, що кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

У випадку, якщо ІКС обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) ІКС комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації ІКС та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації.

Кіберзахист ІКС є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Впровадження організаційних та технічних заходів кібербезпеки в інформаційно-комунікаційній системі повинні забезпечувати:

- формування загальної політики безпеки;
- управління доступом користувачів та адміністраторів до об'єктів захисту;
- ідентифікацію та автентифікацію користувачів та адміністраторів системи;
- реєстрацію подій в системі та їх періодичний аудит;
- мережний захист компонентів системи;
- доступність та відмовостійкість компонентів та інформаційних ресурсів системи;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації;
- визначення умов використання програмного та апаратного забезпечення.

Процес впровадження кібербезпеки в ІКС за Загальними вимогами можна представити моделлю PDCA (англ. Plan-DoCheck-Act – планування – дія – перевірка – коригування), відомий як цикл Демінга (DemingCycle). Ця модель знайшла застосування в нормах ISO, таких як: ISO 9001 – Система управління якістю; ISO 14001 – системи управління навколишнім середовищем; OHSAS 18001 – система управління безпекою і гігієною праці; ISO 27001 – система управління інформаційною безпекою;

ISO 17025 – загальні вимоги, що стосуються компетенції дослідних та калібрувальних лабораторій.

Розглянемо застосування моделі PDCA для процесів системи управління інформаційною безпекою (далі - СУІБ):

- Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (дія) – етап реалізації та впровадження відповідних заходів;
- Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;
- Act (поліпшення) – виконання превентивних і коригуючих дій.

Враховуючи зазначене процес впровадження кібербезпеки за загальними вимогами буде мати наступний вигляд (рис. 1).

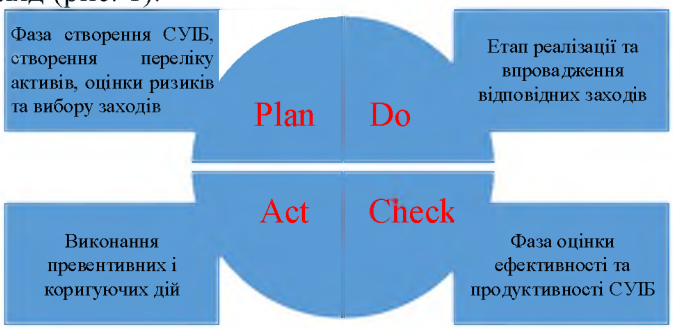


Рис. 1. Процес впровадження кібербезпеки за загальними вимогами

Згідно з міжнародними стандартами ISO/IEC 27001, 27005, управління інформаційною безпекою (кібербезпекою) – це циклічний процес, який складається з:

- усвідомлення необхідності захисту інформації та забезпечення живучості інформаційно-телекомунікаційної системи;
- збору та аналізу інформації про стан забезпечення кібербезпеки в інформаційно-телекомунікаційній системі;
- оцінки інформаційних ризиків;
- планування заходів по усуненню (зменшенню, нейтралізації) ризиків;
- реалізації відповідних механізмів контролю;
- розподілу ролей та відповідальності;
- навчання та мотивації персоналу;
- оперативної роботи по реалізації заходів безпеки;
- моніторингу функціонування механізмів контролю, оцінки їхньої ефективності та визначення відповідних коригуючих заходів.

В цьому ж стандарті визначені принципи управління інформаційною безпекою:

- комплексний підхід – управління повинно охоплювати всі елементи і підсистеми ІКС та враховувати всі ризикоутворюючі фактори;

- відповідність призначенню та завданням застосування Збройних Сил;
- високий рівень керованості (можливість змінювати налаштування та режими функціонування в реальному часі);
- адекватність (релевантність, повнота, достовірність) інформації, яка використовується для управління;
- ефективність – оптимальний баланс між реалізованим ступенем кібербезпеки та затратами;
- безперервність управління;
- замкнений цикл планування, впровадження, перевірки, аудиту і коригування.

Схему процесу управління кібербезпекою в інформаційно-комунікаційній системі можна таким чином (рис. 2.):

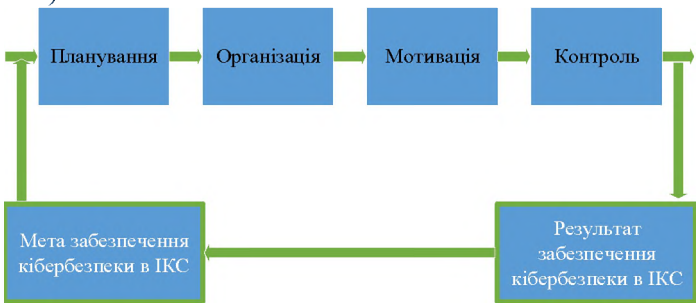


Рис. 2. Схема процесу управління кібербезпекою в ІКС

Основними процедурами управління кібербезпекою в цьому випадку можуть бути:

На етапі планування:
- проектування захищених інформаційно-телекомунікаційних систем;
- розробка політики безпеки;
- планування заходів безпеки;
- вибір засобів забезпечення безпеки;
- планування застосування сил забезпечення кібербезпеки.

На етапі організації:
- реалізація захищених інформаційно-комунікаційних систем;
- реалізація політики безпеки;
- проведення заходів безпеки;
- застосування сил забезпечення кібербезпеки.

На етапі мотивації:
- управління особовим складом сил забезпечення кібербезпеки;
- підготовка особового складу;
- проведення навчань по забезпеченню кібербезпеки.

На етапі контролю:
- контроль проведених заходів;
- аудит кібербезпеки;
- розслідування кіберінцидентів;
- прийняття рішення на коригування заходів забезпечення кібербезпеки.

На даний час в ІКС, які використовуються у Збройних Силах України, впроваджена організаційно-технічна модель кіберзахисту, яка складається з трьох рівнів:
- перший рівень – це організаційно-керуюча інфраструктура кіберзахисту;
- другий рівень – це технологічний рівень або технологічна інфраструктура кіберзахисту, яка складається з сукупності сил та засобів кіберзахисту. Це відповідні технологічні підрозділи кіберзахисту (Кібер-центри) різних секторів. На цьому рівні забезпечується відповідна взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо;
- третій рівень – це базисна інфраструктура кіберзахисту, що забезпечує основні спроможності кіберзахисту.

к.т.н. Штаненко С.С. (ВІТІ ім. Героїв Крут)

ПРОЕКТУВАННЯ АДАПТИВНИХ ВБУДОВАНИХ СИСТЕМ У КОНТЕКСТІ ПІДВИЩЕННЯ ЖИВУЧОСТІ СИСТЕМИ УПРАВЛІННЯ СКЛАДНИМИ ОБ'ЄКТАМИ І ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Вбудовані системи (англ. *Embedded Systems*) представляють собою спеціалізовані мікропроцесорні системи, концепція розробки яких ґрунтується на тому, що такі системи взаємодіють з об'єктом управління або контролю, будучи вбудованими безпосередньо у пристрої, якими вони управляють.

На сьогоднішній день вбудовані системи широко використовуються в різних галузях діяльності таких, як: машинобудування та верстатобудування, авіація, автомобілебудування, атомна енергетика, банківська сфера, військово-промисловий комплекс, а також застосовуються як основа побудови автоматизованих систем управління, засобів автоматичного регулювання та управління технологічними процесами.

Перші вбудовані системи розроблялися в якості спеціалізованих цифрових пристроїв, основу яких складали інтегральні схеми малого та середнього ступеня інтеграції. Однак, з появою мікроконтролерної та мікропроцесорної техніки, а пізніше програмованих логічних інтегральних схем (ПЛІС), поняття вбудованої системи сильно трансформувалося. Так, якщо перші вбудовані системи представляли собою спеціалізовану структуру, яка мала у своєму складі центральний процесор, окремі інтегральні схеми контролерів периферійного обладнання, цифрових запам'ятовуючих пристроїв, то сучасні вбудовані системи реалізують вже технологію *System-on-Chip* (*SoC*) – система на кристалі.

Система на кристалі або *SoC* – це обчислювальна система, архітектура якої розроблена цільовим чином для розв'язання прикладної задачі (або класу задач) і реалізована у вигляді комплексу функціонально спеціалізованих апаратних і програмних компонент на базі конфігурованої мікроелектронної платформи.

На сьогоднішній день проєктування сучасних систем, що використовують технологію *System-on-Chip* засноване на застосуванні високотехнологічних САПР цифрових пристроїв, що вимагає від розробників глибоких знань не тільки цифрової схемотехніки та архітектур обчислювальних систем, але й знання методів синтезу спеціалізованих пристроїв з мікропрограмованим управлінням, знання високорівневих мов проектування та методів контролепридатного синтезу. Тому процес проектування сучасних вбудованих систем – це процес створення власних та використання стандартних цифрових компонентів інтелектуальної власності, які є не тільки схемотехнічним описом, але, по суті, є повноцінними проектними документаціями з функціонального та параметричного моделювання, верифікації та виготовлення із застосуванням сучасних технологій.

Слід зазначити, що в процесі функціонування вбудованих систем можливі збої, відмови, несправності як апаратного, так і програмного забезпечення при виникненні несприятливих впливів (наприклад, іонізуючого та електромагнітного випромінювання, кібератак, шляхом застосування вірусних програм, а саме мережевих черв'яків, вірусів-маскувальників, вірусів-шпигунів, вірусів-зомбі, вірусів-блокувальників, троянських вірусів). Як наслідок таких впливів може бути порушення правильності функціонування або перехід спеціалізованої мікропроцесорної системи в непрацездатний стан, що зрештою може призвести до катастрофічних наслідків у системі управління складними об'єктами та технологічними процесами.

Так, в роботах вітчизняних та іноземних авторів з метою підтримки мікропроцесорної системи в стані правильного функціонування внаслідок несприятливих впливів запропоновано використовувати в якості елементної бази при проєктуванні вбудованих систем інтегральні схеми з програмованою структурою.

Програмовані логічні інтегральні схеми мають характерну особливість, а саме змінювати внутрішні зв'язки між логічними елементами (найпростішими логічними функціями), що дозволяє зробити реконфігурацію внутрішньої структури мікропроцесорної

системи, на відміну від програмованих мікроконтролерів і одноплатних комп'ютерів Raspberry Pi, які мають фіксовану архітектуру та фіксований набір команд. Дана особливість ПЛІС дає можливість, застосовуючи сучасне середовище розробки цифрових пристроїв, наприклад, САПР Intel Quartus Prime, проектувати адаптивні вбудовані системи, в яких реконфігурація архітектури буде проводитися за результатами тестового або функціонального діагностування внаслідок несприятливих впливів.

Якщо розглядати адаптацію вбудованих систем до зовнішніх факторів, то вона безпосередньо пов'язана з такою властивістю складних систем як живучість, під якою розуміється здатність системи протистояти несприятливим впливам і досягати мети функціонування за рахунок зміни поведінки і структури. При цьому підвищення живучості здійснюється розвиненими механізмами розпізнавання, протидії та відновлення, а також спеціальними засобами реконструкції, реконфігурації та реорганізації, які представляють собою адаптивний процес.

Проектування адаптивних вбудованих систем є досить типовою задачею проектування складних систем організаційного типу. При проектуванні таких систем однією з основних задач є синтез структури, що визначає внутрішню організацію та відносно стійкі взаємозв'язки елементів системи. Так, згідно з агрегативно-декомпозиційного підходу під синтезом структури адаптивної вбудованої системи будемо розуміти процес послідовного вирішення системно пов'язаних задач синтезу основних елементів і частин системи. Дані задачі вирішуються ітераційно в силу їхньої взаємопов'язаності, неповноти вихідних даних та необхідності коригування отриманих рішень.

На першому етапі визначається організаційна структура вбудованої системи, виходячи з цілей і стратегій функціонування системи управління складними об'єктами і технологічними процесами. У результаті визначається кількість рівнів ієрархії та вузлів системи, тобто визначається топологічна структура.

На другому етапі визначається функціональна структура, тобто оптимізується розподіл функцій, які виконуються, задач за рівнями та вузлами системи з подальшим перерозподілом при виникненні несприятливих впливів.

На третьому етапі вибирається комплекс обчислювальних засобів, здатних реконфігурувати внутрішню структуру вбудованої системи на рівні елементної бази.

На останньому етапі аналізується динаміка роботи вузлів обраного варіанта структури вбудованої системи з використанням імітаційної моделі.

Розглянемо більш детальніше третій етап, який пов'язаний з реконфігурацією внутрішньої структури вбудованих систем. Слід зазначити, що реконфігурація внутрішньої структури на сьогоднішній день є найбільш перспективним напрямом, з точки зору підвищення живучості вбудованих систем. При цьому в якості елементної бази застосовуються інтегральні схеми з програмованою структурою.

Зазначимо, що принцип реконфігурації вимагає значної надмірності, тому що кожен модуль або вузел вбудованої системи повинен забезпечувати реалізацію будь-якої функції при відповідному сигналі налаштування. Тому кожен модуль, який реалізує в даний момент одну функцію φ_i, повинен мати j-кратну надмірність (j – число всіх модулів функції, яка реалізується).

На рис. 1 представлена структурна надмірність пристрою з j-кратною надмірністю. В результаті використовується лише незначна частина загальної структури модуля. Така надмірність не завжди прийнятна. Більш доцільно включити у роботу всю основну структуру модуля з можливістю виключати окремі його частини у разі виникнення в них несправностей.

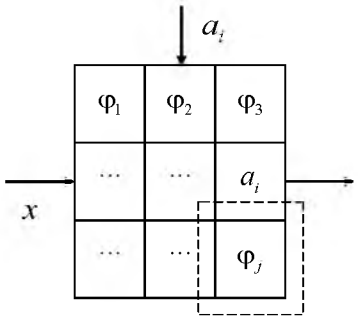


Рис. 1. Структура надмірного пристрою з j – кратною надмірністю

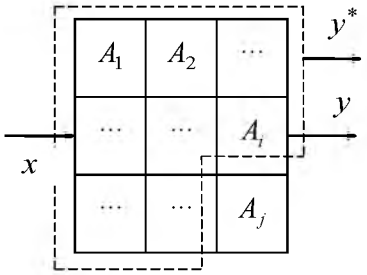


Рис. 2. Блок-схема безнадмірного пристрою з неоднорідними модулями

На рис. 2 представлена блок-схема безнадмірного пристрою з неоднорідними модулями.

Якщо модуль, що містить вузли $A_1 - A_j$, реалізує функцію y, то при виникненні несправності у вузлі A_j і його відключенні, пристрої $A_1 - A_{j-1}$, що залишилися, будуть реалізовувати спотворену функцію y^*. При цьому виникає задача відновлення заданої функції y. Така задача може бути вирішена заміною пристрою A_j резервним, а це по суті – паралельне резервування.

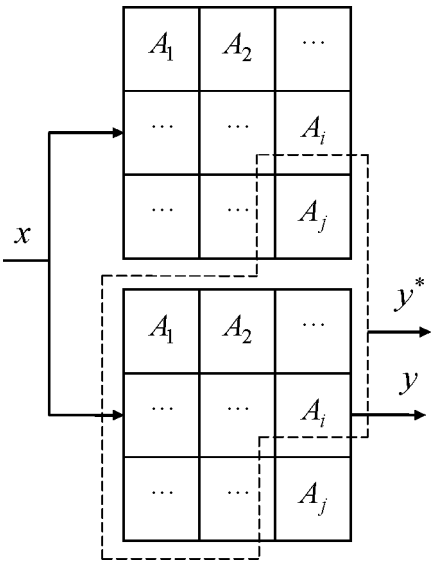


Рис.3. Структура надмірного пристрою з неоднорідними модулями

На рис. 3 зображено структуру надмірного пристрою з неоднорідними модулями. При такій структурі повторна несправність у вузлі A_j модуля A виводить весь модуль з ладу. Для усунення повторної несправності необхідно передбачити n-кратне резервування модуля.

Сформулюємо таку задачу наступним чином: виключення будь-якого з несправних вузлів має бути компенсовано без втручання у внутрішню структуру модуля (у пристроях з недоступною структурою). Один з можливих методів вирішення цієї задачі полягає у відшукуванні такої надмірності структури B_i, яка при підключенні до входу модуля A (при відключеному несправному вузлу A_j) призводить до відновлення функціональних властивостей модуля A (рис. 4).

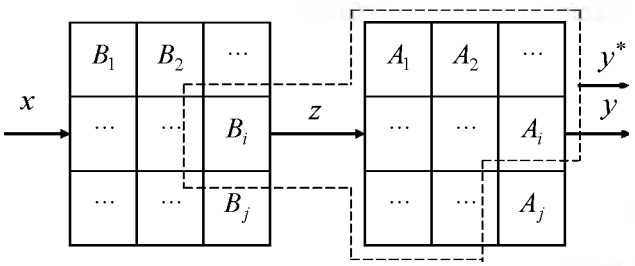


Рис. 4. Структура відновлювального модуля A

В якості прикладу розглянемо цифровий пристрій A_0, що має властивість реконфігурації і реалізує функцію

$$y(x_1, x_2, x_3) = \bar{x}_1 x_2 x_3 \vee x_1 x_2 \bar{x}_3. \quad (1)$$

На рис. 5, а представлена логічна схема цифрового пристрою реалізована в САПР Intel Quartus Prime. Дана САПР є багатофункціональним середовищем проектування, що містить у собі набори утиліт, які дозволяють розробляти, верифікувати та запрограмувати проекти, що реалізують необхідні функції на ПЛІС. На рис. 5, б представлена програма, що реалізує функцію (1) мовою опису апаратури Verilog, яка у вигляді завантажувального файлу ПЛІС буде використовуватися для реконфігурації системи. На рис. 5, в представлена абстрактна RTL-схема на рівні регістрових передач (register-transfer level), яка є обов'язковою для супроводу Verilog коду. А також часові діаграми (рис. 5, г), як кінцевий результат при моделюванні цифрового пристрою з метою перевірки правильності його функціонування.

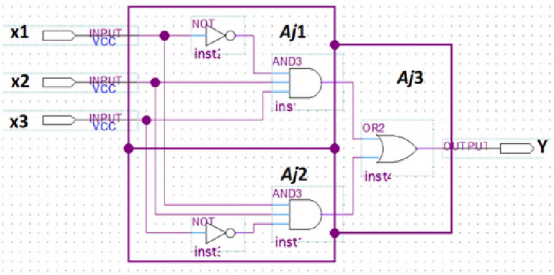


Рис. 5, *а*. Логічна схема цифрового пристрою A_0

```
module ks_1(output Y, input X1, X2, X3);
wire Wire_0, Wire_1, Wire_2, Wire_3;
assign Wire_2 = ~X1;
assign Wire_3 = ~X3;
assign Y = Wire_0 | Wire_1;
assign Wire_1 = Wire_2 & X2 & X3;
assign Wire_0 = X1 & X2 & Wire_3;
endmodule
```

Рис. 5, *б*. Лістінг програми мовою *Verilog*

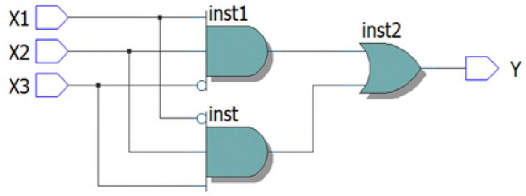


Рис. 5, *в*. Абстрактивна схема цифрового пристрою A_0 на рівні регістрових передач

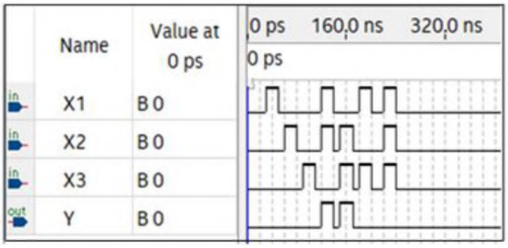


Рис. 5, *г*. Часові діаграми роботи цифрового пристрою A_0

Далі реалізував розглянутий вище принцип реконфігурації отримуємо наступну структуру з надмірністю, яка разом з вузлами вузлами A_{j_2} та A_{j_3}, реалізує задану функцію (1) (рис. 6).

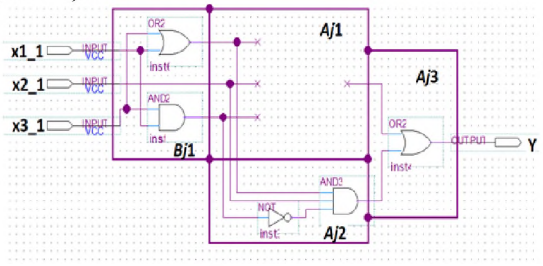


Рис. 6, *а*. Логічна схема надмірного цифрового пристрою, яке складається з вузлів B_{j_1}, A_{j_2}, A_{j_3}

```
module ks_2 (output Y, input X3_1, X2_1, X1_1);
wire WIRE_0, WIRE_1, WIRE_2;
assign WIRE_1 = X1_1 | X3_1;
assign WIRE_0 = X3_1 & X1_1;
assign WIRE_2 = ~WIRE_0;
assign Y = WIRE_1 & X2_1 & WIRE_2;
endmodule
```

Рис. 6, *б*. Лістінг програми мовою *Verilog*

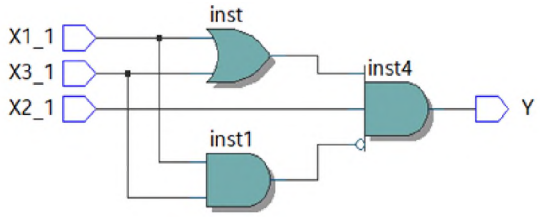


Рис.6, *в*. Абстрактна схема надмірного цифрового пристрою, який складається з вузлів B_{j_1}, A_{j_2}, A_{j_3} на рівні регистрових передач

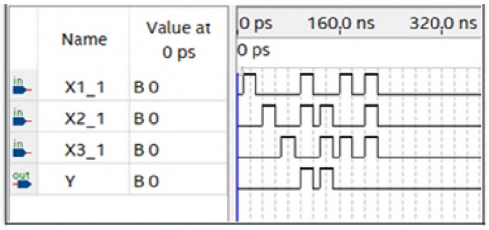


Рис. 6. *г*) Часові діаграми роботи надмірного цифрового пристрою, який складається з вузлів B_{j_1}, A_{j_2}, A_{j_3}

А також надмірну структуру B_{j2}, A_{j1}, A_{j3} (рис. 7).

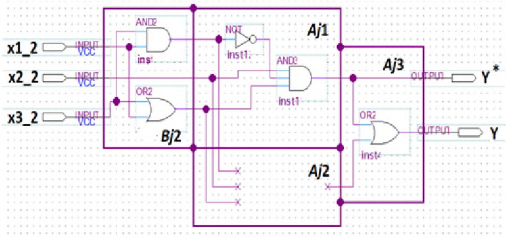


Рис. 7, *а*. Логічна схема надмірного цифрового пристрою, яке складається з вузлів B_{j_2}, A_{j_1}, A_{j_3}

```
module ks_3(output Y, input X3_2, X2_2, X1_2);
wire Wire_0, Wire_1, Wire_2;
assign Wire_0 = X3_2 & X1_2;
assign Wire_2 = X1_2 | X3_2;
assign Wire_1 = ~ Wire_0;
assign Y = Wire_1 & X2_2 & Wire_2;
endmodule
```

Рис. 7, *б*. Лістінг програми мовою*Verilog*

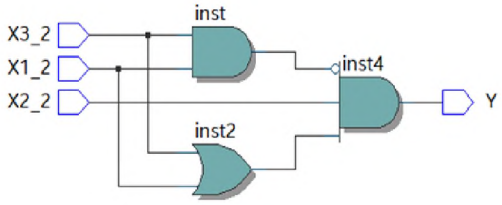


Рис. 7, *в*. Абстрактна схема надмірного цифрового пристрою, який складається з вузлів B_{j_2}, A_{j_1}, A_{j_3} на рівні регистрових передач

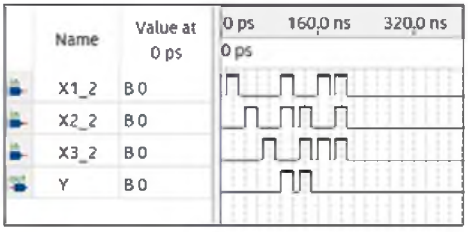


Рис. 7, *г*. Часові діаграми роботи надмірного цифрового пристрою, який складається з вузлів B_{j_1}, A_{j_2}, A_{j_3}

Резюмуючи сказане, можна констатувати, що реалізувавши метод реконфігурації шляхом зміни цифрового пристрою та його надмірної структури за допомогою перепрограмування ПЛІС, ми отримуємо можливість не тільки компенсувати неодноразові несправності на відміну від багаторазового резервування цифрових пристроїв, але й забезпечити відмовостійкість управління загалом.

Висновки. Таким чином запропоновано підхід до проектування адаптивних систем, що базується на можливості спеціалізованої мікропроцесорної системи здійснювати відновлення правильного функціонування внаслідок несприятливого впливу шляхом автоматичної реконфігурації внутрішньої структури за результатами самоконтролю. В основі даного підходу лежить рішення системно ув'язаних задач синтезу основних елементів і частин розподіленої мікропроцесорної системи управління, який включає визначення числа рівнів ієрархії і вузлів системи, розподіл (перерозподіл) завдач за рівнями ієрархії і вузлів системи і вибір обчислювальних систем, здатних реконфігурувати внутрішню структуру на рівні елементної бази. Це дає можливість підвищити живучість не тільки вбудованої системи внаслідок несприятливого впливу, але і всієї системи управління складними об'єктами і технологічними процесами в цілому.

Ph.D Serhiy Hatsenko (NUDU named after Ivan Chernyakhovskyi)
Ph.D Oleksandr Symonenko (MITIT named after Heroes of Kruty)
Andrii Kondrus (MITIT named after Heroes of Kruty)

THE METHOD OF TRAFFIC ANALYSIS OF ANONYMITY USING HIDDEN MARKOV MODEL

Introduction

Tor Browser helps you to protect yourself from "data flow analysis" that threatens personal freedom and privacy, confidentiality of business contacts and connections. This service provides protection by routing your network traffic across a distributed network of servers launched by volunteers from around the world: this does not allow an external observer to track your Internet connection to find out which sites you visit, and also does not allow the site to know your physical location.This program works with many existing applications, including web browsers, instant messaging systems, remote access clients, and other applications using the TCP protocol. This work describes a scenario in which a client interacts with a server through Tor. Assuming that the communication protocol used by the client can be represented by a Hidden Markov Model (HMM), we can derive a model that is an exact representation of the underlying protocol using the time information collected on the server side.

Therefore, ***theaim of this work*** is the traffic analysis of anonymity protocol using Hidden Markov Model (HMM) based on model confidence.

Presentation of the main material of the research

***Z*-test.** Among several classic statistical tests, *z*-test is a simple but widely used statistical test. The rationale for this test: given the random sample size n, a sequence of random variables independent and identically distributed (IID) from an unknown distribution, we are going to make a decision for each value, and this decision will be either correct or not. Consider the distribution of the number of errors that will be made by our classification system.

Or, since the statistics *z* follows the standard normal distributions, if the null hypothesis is correct, the decision to reject the null hypothesis can also be made by comparing the statistics *z* with a critical value without converting it to p-value.

Hidden Markov Model. The standard Hidden Markov Model (HMM) is N-Markov chain observed at discrete points in $t = 0,1,2....$ Let us assume that $S = \{1,2,...,N\}$ represents the space of the final state if we use a random variable S_t to indicate the state of the HMM at the time t, $S_t = s$ means that the HMM is in the condition of $s \in S$ in time step t. However, S_t can`t be observed directly. Instead, we see one way out.In this paper, we consider the problems of HMM inference and a specific inference algorithm is the causal splitting restoration algorithm (CSRA). This approach of the HMM creates state machines deterministic at the transition exit, i.e. when each observation is displayed in no more than one transition, leaving the state. In addition, the main Markov chain HMM generated using the Shalizi method when all transition states are removed.

Partially Observable Markov Decision Process. In the language of stochastic control, Partially Observable Markov Decision Process (POMDP) are control problems with partial observation. They usually simulate stochastic environments with hidden processes. By summarizing the Markov decision process (MDP) and providing greater uncertainty, the POMDP provides a more powerful formalism for modeling realistic problems, especially for managing systems with noisy data or limited sensitivity.The goal of the POMDP study is to find a sequence of actions known as the policy that makes the system work as agents want. A policy is measured by a compensation function, which is a mathematical function of immediate remuneration. The goal of the agent is to optimize the compensation function.

Decentralized POMDP. When decision making becomes a collective work in which several agents need to be coordinated without effective communication and even unclear about their own local situation, the decentralized as an extension of POMDP to the case of several agents, DC-POMDP is a more general and more powerful modeling tool. However, the DC-POMDP solution

usually leads to excessive computational overhead.But joint actions affect both the dynamics and the global reward.

Final State Controller (FSC). Although any POMDP policy may be represented by a policy schedule, for some policies of an infinite horizon, infinite policy schedules may be required. Therefore, most policy-based algorithms limit their search to finite political graphs. Since the concept of FSC is not accepted. The transition of the internal state is probabilistic and is determined by recent history.

Sequential Quadratic Programming (SQP). SQP is one of the most successful methods for solving problems of nonlinear limited optimization. It consists of a set of algorithms, not just one algorithm and is based on a deep theoretical foundation. SQP has demonstrated excellent performance in solving general problems of large-scale non-linear programming. In this section, we look at the following NLP (natural language processing) problem.SQP solves NLP to convert it into a series of problems with quadratic programming (QP). At each iteration, the original NLP is reformulated as a subtask QP, linearizing the constraints and replacing the objective function $f(x)$ with its local quadratic approximation. There are many NLP for which individual SQP methods exist to solve them. This NLP include unconditional optimization systems, linearly limited optimizations and non-linearly limited optimizations. We speak POMDP as NLP and rely on SQP tools to find solutions.

Anonymity Protocol Analysis. To use the z-test, let us offer a simple algorithm for operational testing of the sequence of observations. The algorithm determines whether the built model will statistically represent the data flow in the collection process. First, we collect a sequence of observational data y of some length and build a model from the collected data. With a built model, we define z-statistics and find if experimental statistics provides $100 \cdot (1-\alpha)\%$ confidence that the transition with probability ε does not occur. If y is not long enough, we will not be able to build a model from the data; it is necessary to collect additional data. The algorithm is presented below.

Protocol Detection. Now we use the model trust approach presented above to determine the protocol that the sender uses when talking to a client over the Tor network, collecting time intervals between packets on the client. This method links inter-packet delays with HMM transitions. In other words, the time delays between successive packets will be our observations of the main process. This is the behavior that we expect in actual protocols that the packet time will be associated with the processing required by a particular task in this process.

An overlay network is a logical network connected by virtual circuits on top of a physical network. Links that connect individual systems in the overlay network are implemented as "tunnels" through the core network. Sent packets are encrypted multiple times so that they remain logically separate from normal traffic. The connection between the client and the entry node is first established using TLS/SSLv3 for authentication and encryption. After creating the first connection, the path extends to the second and third nodes in a similar way. Using this incremental path-building project, the client sets the session keys with each subsequent node independently. The final node of the scheme, known as the output node, is selected to ensure, at best, support for connections to the destination.

Conclusion

This scientific work analyzes the traffic of the anonymity protocol using a hidden model of the model based on the Markov model, reveals its main features.Thus, the work describes the temporal side of the synchronization channel attack to detect a communication protocol tunnelled through Tor. Model trust algorithm is applied to the implementation of the attack. A proof-of-concept experiment on our private Tor network showed that a model could successfully be reconstructed from inter-packet timings, and also proved the practical application of the model trust algorithm.The direction of further research should be considered the development of methods for increasing the confidentiality of traffic in public networks.

PhD S. Khmelevsky (KhNAFU)
I. Tupitsya (KhNAFU)

THE METHOD OF MARKER ENCODING IRREGULAR CODE STRUCTURES TO INCREASE THE RELIABILITY OF VIDEO INFORMATION IN INFOCOMMUNICATION SYSTEMS OF UNMANNED AIRCRAFT

Today, the rapid pace of digitization of the information space is accompanied by the active use of video information support. This is due to the fact that the video information resource is used to provide departmental bodies with up-to-date and complete information (about the state of state borders - border systems of photo and video surveillance), interaction of headquarters with subordinate units (video conference communication), remote monitoring of objects of critical infrastructure and conducting terrain reconnaissance on the positions of enemy units (aerial monitoring using unmanned aerial vehicles (UAVs)).

Thus, the active use of UAVs is associated with the need for prompt response to crisis situations arising in society and the state as a whole, dynamic changes in the location of enemy units. In connection with this, the requirements for video information resources are increasing from the point of view of ensuring their completeness (integrity), relevance and reliability. A problematic aspect of the implementation of the latter is the effects of interference in data transmission channels using wireless technologies in conditions of bandwidth limitations.

In connection with this, increasing the reliability of video information, in the conditions of using wireless communication technologies, is an urgent scientific and applied task.

The purpose of the work is to develop the technology of marker coding of uneven code structures to increase the reliability of video information in the information communication systems of unmanned aerial vehicles.

It should be noted that modern video data encoding technologies are implemented according to the principles (processing stages) that make up the toolset of the basic JPEG platform. The basis of the algorithms of the specified family is a statistical approach used at the final stage of data processing. The statistical approach refers to the use of a synthesis of statistical coding methods - the group coding method and the Huffman method.

The result of the process of statistical coding of video data is the formation of the original code sequence consisting of non-uniform code structures, the main feature of which is the property of prefixity.

A number of experimental studies conducted show that in the conditions of the impact of errors in the process of video image reconstruction, the use of these technologies does not allow to localize the impact of errors, but leads in most cases to the destruction of the information resource [1-2].

To increase the reliability of video data in the conditions of ensuring delivery efficiency, it is proposed to use the method of marker coding of uneven code structures formed in the process of statistical coding of data obtained as a result of data restructuring.

Unlike the existing ones, the developed way of forming markers is implemented by using a statistical approach to reduce code redundancy. This makes it possible to ensure the localization of the impact of errors within the boundaries of uneven code structures and, as a result, to increase the reliability of the data.

REFERENCES

1. Тупиця І. М., Кібіткін С. О., Сухотеплий В. М., Непокритов Д. М., Конов Д. В. (2022). Метод реконструкції відеозображень для підвищення ефективності доставки в інфокомунікаційних системах аеросегмента. Вісник Вінницького політехнічного інституту. 2022. № 4(163), С. 72–82. https://doi.org/10.31649/1997-9266-2022-163-4-72-82.

2. Karlov, D., Tupitsya, I., Parkhomenko "Methodology of increasing the reliability of video information in infocommunication networks aerosegment", Radio Electronics, Computer Science, Control, No. 3(2022), pp. 120-132. DOI:https://doi.org/10.15588/1607-3274-2022-3-12.

PhD S.Khmelevsky (KhNAFU)
I.Tupitsya (KhNAFU)
O.Pershin (KhNAFU)

THE CONCEPT OF FORMING A HIDDEN DATA TRANSMISSION CHANNEL IN SPECIAL PURPOSE INFORMATION AND TELECOMMUNICATION NETWORKS

To date, the conduct of hostilities on the territory of Ukraine is accompanied by a dynamic increase in confrontation in the information space. In connection with this, the requirements for the information resource, which is transmitted in special purpose information and telecommunication networks (ITN SP), from the standpoint of ensuring information security, are increasing. The main ones are the following:

- ensuring the integrity of the data transmitted to the ITN of the SP;
- ensuring data confidentiality, i.e. access to service information (SI) only to authorized users.

In order to fulfill the above requirements, cryptographic methods of information protection are actively used, which allow to ensure the required level of information security. However, along with the advantages, the use of this approach has a number of problematic aspects:

- the enemy knows that service information is being transmitted and as a result he directs all the power of computing resources to decrypt the codegram;
- complex algorithmic implementation of cryptographic protection methods, which requires the involvement of significant computing resources;
- the cost of technical means of cryptographic protection of information, which makes it impossible to use them at all levels of management.

In connection with the problem of using cryptographic tools and methods to ensure the necessary level of information security, the issue of finding new approaches that will allow to fulfill the above requirements becomes urgent.

Therefore, increasing the information security of data transmitted in special purpose information and telecommunication networks from the standpoint of ensuring the required level of integrity and confidentiality is an urgent scientific and applied task.

The purpose of the work is to develop a model for hiding service data transmitted in special purpose information and telecommunication networks to ensure the necessary level of integrity and confidentiality of information in the conditions of ensuring the simplicity of algorithmic implementation.

For this purpose, it is proposed to use a fundamentally new approach for special purpose information and telecommunication networks - steganographic, the essence of which is to hide the very fact of the existence of secret information in the transmitted information resource.

To organize a hidden data transmission channel, it is proposed to use a synthesis of steganographic hiding methods and cluster analysis of the original container. It is suggested to use a video information resource as the container of the original. Cluster analysis of data is proposed to be carried out by identifying patterns in the binary representation of the original container. This will make it possible to create conditions for delimiting access to official information while maintaining its integrity.

REFERENCES

1. Khmelevskiy, S., Tupitsya, I., Mahdi, Q. A., Musienko, O., Parkhomenko, M., Borovensky, Y. (2021). Development of the external restructuring method to increase the efficiency of information resource data encoding. Information Processing Systems, 3(166), pp. 52-61. https://doi.org/10.30748/soi.2021.166.06.

2. Karlov, D., Tupitsya, I., Parkhomenko, M., Musienko, O. andLekakh, A. (2022) "Compression Coding Method Using Internal Restructuringof Information Space", International Journal of Computing, 21(3), pp. 360-368. doi: 10.47839/ijc.21.3.2692.

Ph.D S.Vasylenko (ISCIP of Igor Sikorsky KPI)
Ph.D Y.Zinchenko (ISCIP of Igor Sikorsky KPI)

METHOD OF MANAGEMENT OF THE SECURITY STATUS OF THE AUTOMATED PROCESS CONTROL SYSTEM OF CRITICAL INFRASTRUCTURE FACILITY

In order to speed up the decision-making process, as to well as reduce the negative influence of operators on management processes, modern industrial enterprises are increasingly automating the processes of managing technological equipment. Management of such systems is carried out with the help of considered the automated process control system (APCS), which differ from ordinary corporate networks by the presence of specialized technical and software tools.

In the event that an industrial enterprise, by the type of its main services, belongs to critical infrastructure objects, the automated technological process management system of such an enterprise becomes an object of critical information infrastructure facility of critical infrastructure facility (CIIF of CIF) and needs improvement of the information protection system.

At the same time, the APCS protection system should be built based on the need to respond to a complex of threats and their coordinated implementation and be aimed at ensuring the stability of the operation of the CIF [1-2].

The purpose of the work is to determine the rules for making decisions regarding the detection of cyber incidents and the selection of means of protection against the influence of cyber attacks on the APCS of CIF.

A logical inference mechanism is used to describe the base of system input parameters used to detect an attack. Detection of signs of a change in the system state is carried out on the basis of a comparison of the input parameters of the system with the reference ones (obtained at the commissioning stage). At the same time, attacks can be defined as:

$$X = X_1 \cup X_2 \cup ... \cup X_n,$$

where $X_1 = \{x_i(t), i = \overline{1, m}\}$ – set of parameters on the 1st level;

$X_2 = \{x_i(t), i = \overline{1, m}\}$ – set of parameters on the 2nd level;

$X_n = \{x_i(t), i = \overline{1, m}\}$ – set of parameters at the m-th level.

The choice of means of protection (MP) of the system with a complete description of the automatic control system is carried out on the basis of dynamic programming, taking into account the strategies of influence on it.

The probability of carrying out j_z cyber attack on a set of objects l can be defined as:

$$P(j_z, l) = \prod_{v=1}^{l} P_v^{j_z}.$$

The management decision regarding the application of specific MP $U_k = U(t) = \{u_1, ..., u_n\}$ is made on the basis of a comparison of the received data on the state of security of the system $X(t)$ and the information available in the database about the previously adopted decisions $U_{k-1}, U_{k-2}, ..., U_{k-l}$ and implemented options for influencing security violations Λ and is described as:

$$X(t)=\{x_1,...,x_8\},\quad U=\{U_1,...,U_k\},\quad \Lambda=\{\Lambda_1,...,\Lambda_k\},$$

where $k=1,2,...,N$.

The means of protection U_k used at any of the steps affect possible security violations $\Lambda_{k+1},\Lambda_{k+2},...$ at the following steps, and therefore the state of security of the APCS as a whole [14-15].

The rule on the application of protective measures based on the received data up to and including the k-st step can be presented in the form of a probability measure that depends on the state of system security and the set of previous management decisions up to and including the k-st step:

$$p_k=p_k(U_k\mid X_k,U_{k-1}).$$

For a multi-step procedure of finding the optimal sequence of making a decision regarding the use of protection means, dynamic programming methods can be used in a general stochastic form. The optimal Bayesian decision-making rule at the k-st step determines the optimal sequence of using measures to combat violations by making management decisions:

$$\min_{U_k} R_k(U,X_k)=\min_{U_k} M\{g(U_k,\Lambda_k,X_k))\mid X_k,U_k\},$$

where $R_k(U,X_k)$ – posterior risk function for a set of decisions and observations;

$M\{g(U_k,\Lambda_k,X_k))\mid X_k,U_k\}$ – mathematical expectation of the security state change function.

The proposed method of managing the state of security against cyberattacks on the APCS of CIF allows management decisions to be made regarding the use of protective measures to increase the level of security of information resources circulating in the system, with a large number of input parameters of cyberattacks based on dynamic programming.

Conclusions

In the work aimed at determining the decision-making rule for the detection of cyber incidents and the selection of protection means for the APCS of CIF against the influence of cyber attacks, the use of an optimal Bayesian decision-making rule is proposed, which will allow at any k-st step, based on the study of changes in system parameters, to carry out detection cyber incident and make the necessary management decisions regarding the application of specific means of protection.

REFERENCE

1. O. M. Sukhodolia "Zakhyst krytychnoi infrastruktury v umovakh hibrydnoi viiny: problemy ta priorytety derzhavnoi polityky Ukrainy", *Strategic priorities,* Vol. 3, p. 62-76, 2016. [Online]. Avaliable: URL : http://nbuv.gov.ua/UJRN/spa_2016_3_10. Accessed on: May 15, 2022.

2. Bazovi rekomendatsii z kiberbezpeky promyslovykh system upravlinnia dlia viddiliv ASU TP (August 2017), *TK 185 "Promyslova avtomatyzatsiia". Hrupa "kiber-bezpeka v ASU TP".*

3. S. Storchak, S. V. Salnyk "Metod otsiniuvannia rivnia zakhyshchenosti merezhevoi chastyny komunikatsiinoi systemy spetsialnoho pryznachennia vid kiberzahroz", *Information processing systems,* № 3(158). p. 98-109, 2019. doi:10.30748/soi.2019.158.12.

4. S. Storchak "Metod otsinky zakhyshchenosti informatsii na osnovi bahatokrokovykh protsesiv pryiniattia rishen", *Skhidno-Yevropeiskyi zhurnal peredovykh tekhnolohii. Fizyko-tekhnolohichni problem radiotekhnichnykh prystroiv, zasobiv telekomunikatsii, nano- imikroelektronik.* № 2(66), p. 82-85, 2013.

Zaluzhnyi O.V. (MITIT n. Heroiv Krut)
Yurchenko O.V. (MITIT n. Heroiv Krut)

APPLICATION OF MACHINE LEARNING ALGORITHMS FOR THE CLASSIFICATION OF THE MODULATION OF THE INCOMING RADIO SIGNAL

Modulation and demodulation are key parts of all analog or digital communication systems. Nowadays more and more modulation types are used and an automatic way of modulation classifying of the incoming radio signal is an important part of every system. This is very useful for cognitive radio, spectrum surveillance and management, radio electronic reconnaissance etc. Solving the modulation classification problem is the subject of active scientific research. But the application of machine learning (ML) algorithms to solve this problem remains underexplored. Therefore, the development of the ML model for the classification of the modulation of the incoming radio signal using different learning algorithms is an important task.

The purpose of the research is to analyze the effectiveness of using machine learning algorithms for automatic classification of the modulation of the incoming radio signal.

In the proposed ML model the I and Q (In-phase Amplitude, Quadrature Amplitude) coordinates of signal constellation points are used as the dataset. The dataset contains samples of some basic modulation types, generated in MATLAB with a random signal-to-noise-ratio in the range [-20, 20] dB. Developed ML model used eight datasets for different modulations schemes such as PAM4, PAM16, QPSK, PSK8, APSK32, APSK64, QAM16, QAM32, QAM64. All datasets were in "csv" format. The names of all datasets are related to the used modulations schemes (modulation schemes are classes in the ML model). The first row of all datasets contains the names of the constellation image coordinates (these are features in ML model), modulation schemes and the SNR. The next lines contain the values of the I and Q coordinates. An example dataset is shown in the Figure 1.

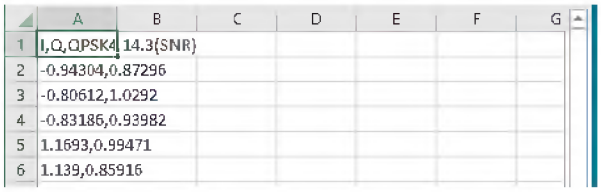


Figure 1. An example of dataset

Random forest, decision tree, naive Bayes, support vector machine and k-nearest neighbors (KNN) algorithm were used to select the best algorithm for solving the problem. ML models were tested using different algorithms.

Value of precision, recall and f1-score received and confusion matrix was constructed. The best results were obtained using the KNN algorithm. The results of model testing are illustrated in the Table 1 and the Figure 2.

Table 1

Value of precision, recall and f1-score received using KNN algorithm

Modulation tips	Encoded labels	Precision	Recall	F1-score
APSK32	0	0.86	0.93	0.89
APSK64	1	0.82	0.68	0.74
PAM16	2	0.78	0.94	0.85
PAM4	3	0.77	0.66	0.71
PSK8	4	0.82	0.77	0.79
QAM16	5	0.63	0.75	0.69
QAM32	6	0.64	0.55	0.59
QAM64	7	0.62	0.65	0.63
QPSK	8	0.70	0.64	0.67

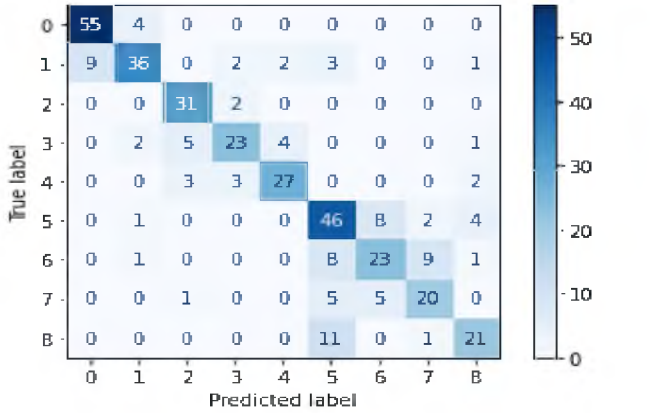


Figure 2. Confusion matrix for KNN algorithm

Thus, to solve the problem of modulation classification, it is advisable to use the KNN algorithm for the ML model. The proposed model is experimental, but it allows to classify the modulation of the received signal with an accuracy of 0.74 at SNR in the range [-20, 20] dB. For better results, larger data sets should be used to perform outlier removal and dimensionality reduction procedures.

The further direction of research is the use of unsupervised learning algorithms to solve the problem of modulation classification.

к.е.н. Аверічев І.М. (ДУТ)
Чуприна М.Ю. (ДУТ)

ЗАСОБИ ПІДВИЩЕННЯ ЖИТТЄЗДАТНОСТІ ВЕБ-САЙТУ ЯК ІНФОРМАЦІЙНОГО ПРОДУКТУ

На даний час можна з упевненістю стверджувати, що сучасне суспільство поступово перетворюється у „інформаційне" суспільство. При цьому виявляються характерні риси даного суспільства, а саме: відзначається зниження ролі матеріального виробництва, розвиток сектора послуг і зростаюча роль інформації.

Відображаючи реальну дійсність, інформація інтегрується в усі напрямки діяльності держави, суспільства, громадянина. З появою нових інформаційних технологій, основою яких є впровадження засобів обчислювальної техніки, зв'язку, систем телекомунікації, інформація стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, громадських організації та громадян. Від її якості та достовірності, оперативності одержання залежать численні рішення, що приймаються на різних рівнях – від глави держави до громадянина.

Існує багато задач, що є нерозв'язаними для інформаційного продукту (ІП). Нерозв'язаними задачами у веб-середовищі є наступні:

a) для сайтів загального характеру:

- аналіз веб-сайтів з точки актуальності інформації чи публікацій;
- дослідження розвитку, використання, вдосконалення веб-сайтів;
- захист персонального інформаційного наповнення та обмеження щодо використання інформаційного продукту, взятого з інших джерел (наприклад з інших веб-сайтів);
- дослідження відношень між розробниками, замовниками та користувачами (оскільки інколи ці відношення можуть співпадати, тобто одна людина може бути одночасно, наприклад, власником і розробником веб-сайту, або розробником одного веб-сайту та користувачем іншого);
- пошук оптимального рішення між розробником інформаційного продукту з одного боку і користувачами цього ІП – з іншого.

b) для сайтів дистанційних послуг (дистанційної освіти):

- уніфікації та інтеграція даних в ІП різних дистанційних технологій навчання, формулювання сфер використання (функція корисності);
- координація та управління навчальною інформацією (з врахуванням масиву інформації, що отримується з різних джерел);
- визначення впливу можливих факторів ризику на поведінку нових розподілених ІП з навчальної інформацією, розроблення методів прийняття рішень щодо поведінки таких ІП;
- структуризація методів та засобів обміну даними, доступ до інформаційних ресурсів, ефективне використання електронних форм представлення інформації в Інтернет-орієнтованих освітніх проектах з дистанційною формою подання (відео курси).

Мета роботи полягає у розвитку підходів до подовження тривалості життєвого циклу та підвищення життєздатності веб-сайту як інформаційного продукту (ІП) шляхом розроблення методів і засобів побудови послідовності зміни його станів.

Життєздатність – міра, з якою ІП використовується в певній предметній області для досягнення конкретної мети з відповідною ефективністю, продуктивністю, задоволенням потреб на визначених інтервалах часу. Життєздатність інформаційного продукту залежить від часу його створення, метаданих, характеристик, при яких подальше використання його неможливе або небажане через зниження його життєздатності.

Веб-сайт – це інформаційний продукт, що є результатом функціонування інформаційної технології (комбінація програмних засобів і даних). Веб-сайт має власну («фізичну») адресу, довідкові і регулярні дані, файли тощо (зокрема, так званий «словник»).

Веб-сайт як інформаційний продукт може містити: текстові файли, електронні таблиці, графічні дані, бази даних чи сховища даних, веб-сторінки.

ІП складається з інформаційних ресурсів, інтелектуальних ресурсів, метаданих про цей ІП. Інформаційний ресурс – сукупність структурованих даних для отримання достовірної інформації, фіксована на матеріальному носії. Інформаційним ресурсом веб-сайту як інформаційного продукту є його наповнення (контент). Інтелектуальні ресурси (інформаційно-інтелектуальні ресурси) – сукупність об'єктивних форм інформації чи знань, отриманих в результаті інформаційно-технологічних, науково-виробничих, організаційно-управлінських, маркетингових, фінансових, юридичних тощо методів, технологій, засобів, різних форм подання завдяки інтелектуальній праці. Інтелектуальними ресурсами є програмні модулі, структурні схеми, технічні характеристики ІП тощо. Метадані про ІП – опис методів та засобів створення інформаційних продуктів (кількості ІР, технічного рішення тощо), структури його даних:

Складові веб-сайту як інформаційного продукту подано на рисунку 1.1.

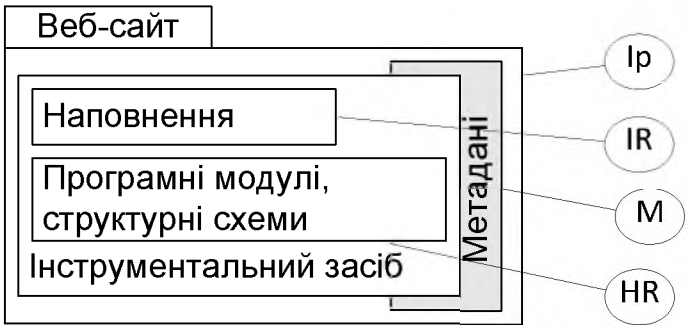


Рисунок 1. Складові веб-сайту як інформаційного продукту

Інформаційний продукт має три складові: інформаційну, технічну, соціальну (рисунок 2.1): інформаційна складова включає опис принципів і методів створення; технічна – засоби створення, з допомогою яких реалізується ІП; соціальна – сферу застосування (призначення, вік користувачів, для яких ІП був створений).

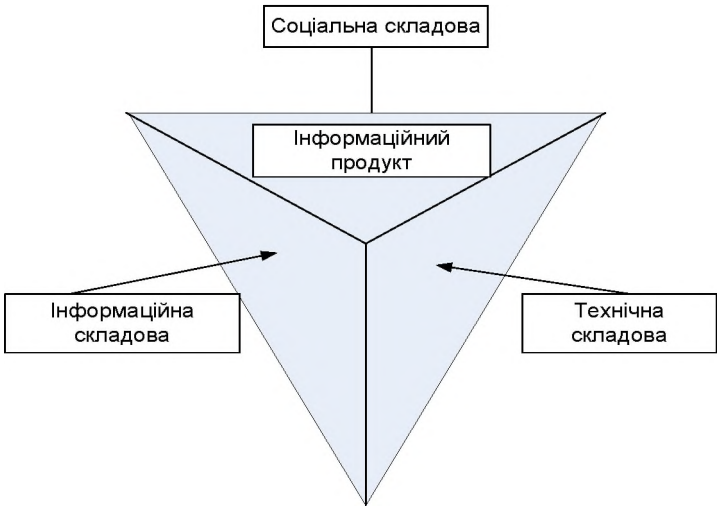


Рисунок 2. Складові інформаційного продукту

Виділяють два варіанти експлуатації інформаційних продуктів: з одного боку, використання інформації у промисловості та соціальній сфері, а з іншого – у високоорганізованих індустріальних методах здійснення інформаційних процесів.

Інформаційне суспільство (ІС) – суспільство, в якому інтеграція і маніпулювання інформацією відбувається завдяки інформаційному процесу і має істотний вплив на всі

сфери діяльності людини, зокрема – економічну, культурну, наукову тощо. Суб'єктами інформаційного суспільства є користувачі інформації.

Створення інформаційних продуктів зумовлено взаємопроникненням двох значних соціально-економічних процесів – індустріалізації інформатики та інформатизації суспільства, що створило важливі передумови для формування та реалізації нової моделі розвитку економіки і суспільства, становлення постіндустріальної цивілізації. Тобто, інформаційний продукт отримується в ході інформаційного процесу, застосованого до інформаційних ресурсів.

Процес прийняття рішень щодо підвищення життєздатності ІП (ППР ІП) є результуючим процесом отримання, переробки і передачі знань, який починається з надходження до комунікатора ІП (наприклад, розробника) первинних відомостей, генеруванням інформації для досягнення конкретної мети, перетворенням відомостей в окремі елементи ІП, і закінчується створенням нових ІП з врахуванням вимог комуніканта (користувача) інформаційного суспільства. Основною задачею процесу прийняття рішення щодо підвищення життєздатності ІП є створення стратегій, направлених на адаптацію продукту до вимог користувачів в умовах ринку, виокремлення його з поміж інших ІП за рахунок унікальних характеристик, умов його отримання чи сервісного обслуговування. Дія стратегій передбачає:

- зміцнення позицій ІП на ринку за рахунок покращення якісних характеристик;
- зміну (часткову зміну) сфери використання ІП;
- внесення змін в сприйняття ІП користувачами за рахунок формування нових критеріїв оцінки ІП;
- підвищення життєздатності ІП.

В інформаційному суспільстві – інформація – це володіння знаннями. Вона впливає на життєздатність ІП, його використання, підвищення ролі технологій, сприяє покращенню якості інформаційних послуг. Управління інформацією є, по суті, управлінням станами будь-якого інформаційного продукту, зокрема, веб-сайту.

Веб-сайт, поданий як інформаційний продукт, може містити дані – тобто відомості, подані у певній знаковій формі, придатній для передавання, інтерпретації та опрацювання людиною або автоматизованою системою чи пристроєм. Дані, що використовуються, називають інформативними та надають інформацію лише в момент їх використання.

Для прийняття рішень стосовно життєздатності веб-сайту як інформаційного продукту необхідно, щоб дані, які надходять із різних джерел, задовольняли таким вимогам:

- були своєчасними, повними та несуперечливими;
- були інформативними, оскільки в подальшому вони використовуватимуться для прийняття рішень;
- були однакової структури – для можливості завантажити їх у однорідне сховище даних (СД) та проаналізувати;
- зберігалися в однакових моделях даних та були незалежними від платформи розроблення – для використання цих даних в інших засобах (методах, модулях).

Таким чином, для вирішення задачі підвищення життєздатності веб-сайту як інформаційного продукту пропонується комплексний підхід, який включатиме в себе:

- уточнення класифікаційних ознак ІП, за якими слід віднести його до конкретного класу;
- формування значущих характеристик і факторів впливу, та їх вплив на життєздатність веб-сайту як інформаційного продукту;
- ранжування (присвоєння коефіцієнта важливості) значущим характеристикам веб-сайту як інформаційного продукту;
- формування універсальної матриці інформаційних зв'язків на основі сценаріїв зміни станів інформаційних продуктів.

Андрушко М.В. (ДНДІ ВС ОВТ)
к.т.н. Аркушенко П.Л. (ДНДІ ВС ОВТ)
Кузьміч О.Є. (ДНДІ ВС ОВТ)
Андрушко А.М. (ДНДІ ВС ОВТ)

АНАЛІЗ ОСОБЛИВОСТЕЙ ТЕЛЕМЕТРИЧНИХ СИСТЕМ СУЧАСНИХ ПРОМИСЛОВИХ ОБ'ЄКТІВ

Постановка проблеми.

Метою статті є аналіз особливостей існуючих та перспективних інформаційно-вимірювальних радіотелеметричних систем сучасних промислових об'єктів для забезпечення якісного процесу організації проведення випробувань дослідних зразків новітнього озброєння та військової техніки.

Основні положення.

Промислові об'єкти, як правило, характеризуються складністю і комплектністю технологічних процесів, а також просторовим розміщенням окремих функціональних блоків і систем по відношенню до центру управління.

Сучасна система контролю промислового об'єкту являє собою автоматизовану систему контролю стану і управління технологічним процесом з використанням сучасних методів вимірів, засобів збору та обробки, аналізу і подання даних про хід процесу, архівування та функцій управління.

Основу інформаційно-аналітичного комплексу практично для будь-якого складного та динамічного технологічного процесу і промислового об'єкту доцільно реалізувати в вигляді системи телеметрії.

На телеметричні системи промислового об'єкту покладаються наступні функції:

– вимір групи параметрів, які характеризують стан окремих вузлів і деталей, а також по можливості безпосередніх процесів;

– подання результатів вимірів в формі, зручній для подальших операцій;

– збір даних про стан окремих блоків і вузлів промислового об'єкту та поточні параметри процесу;

– обробка даних з метою отримання інформації про стан окремих вузлів промислового об'єкту та характеру перебігу процесу в окремих його перетинах;

– ведення архіву даних про процеси з метою ретроспективного аналізу ходу перебігу їх в промисловому об'єкті;

– генерування сигналів, попереджувальних про порушення режиму та виникнення аварійної ситуації;

– вирішення діагностичних задач з метою визначення та своєчасної локації міста виникнення порушення режиму, змінюючого характер протікання процесу;

– по можливості телеметрична система також повинна забезпечувати прийняття рішення про управлінський вплив у випадку виявлення тенденції відхилення параметрів від норми.

Сучасна система телеметрії повинна мати вихід на локальні регулятори, призначені для управління технологічним процесом. Система повинна виробляти сигнали різноманітних блокувань, відключень, тощо у випадках появи нештатних та аварійних ситуацій.

Для забезпечення більш високої надійності комплексу і достовірності отримуваної інформації, враховуючи специфіку процесів, неперервність та довготривалу роботу промислового об'єкту і окремих груп обладнання, повинна бути забезпечена апаратурна та інформаційна надлишковість.

Система контролю для промислового об'єкту це автоматизована система телеметрії, сумісну з системою управління процесом розвитку і режимами роботи окремних технологічних

блоків та вузлів. Крім того, в сучасних умовах система управління в тій чи іншій мірі

пов'язано з використанням інтелектуальних систем.

Системи телеметрії разом з системами та пристроями управління створюють систему, яка може дуже ефективно вирішувати, як задачу достовірного контролю стану технологічного процесу і обладнання, так і задачу ефективного управління всім технологічним комплексом.

Розгляд якісно нового системно-інтегрованого підходу до регулювання і супроводження процесів забезпечення безопасної та ефективної експлуатації всього промислового комплексу на основі аналізу об'єктивної експлуатаційно-промислової інформації,отриманої шляхом інтеграції інформаційних потоків гетерогенних інформаційних систем.

Разом з тим, зазначимо що в останні роки відмічається поява широкого класу нових матеріалів і як наслідок удосконалення давальної апаратури. В області розробки програмних засобів спостерігається тенденція розробки універсального інструмента, який дозволяє фахівцю швидко та ефективно вирішувати проблеми збору, обробки і подачі інформації та управління промисловими об'єктами, а також пристосуватися до особливостей процесу.

Світові лідери в цій галузі постійно відслідковують останні досягнення в області давальної апаратури та обчислювальної техніки, особливо мікропроцесорної, постійно працюють над удосконаленням усіх аспектів технологій для телеметрії технічних об'єктів.

В розробці концепції та при проектуванні системи телеметрії для промислових об'єктів спостерігається стійка тенденція на застосування універсальних апаратних і програмних засобів. Універсальність яких з тенденцією обміну особливостей технологічного процесу і особливостей обладнання та максимальної адаптації системи до цих особливостей.

Таким чином, кінцевою метою такого з'єднання універсальності і спеціалізації є максимальна ефективність функціонування промислового об'єкту та його конкурентоспроможність.

Висновок.

З огляду на наведене є подальша необхідність та доцільність в удосконаленні системи контролю якості технологічного процесу з урахуванням сучасних досягнень мікропроцесорної апаратури та сучасності програмних продуктів з застосуванням перспективних інформаційно-вимірювальних радіотелеметричних систем, що в свою чергу вплине на ефективність проведення випробувань дослідних зразків озброєння та військової техніки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основы военно-технических исследований. Теория и приложения. Система полигонных испытаний вооружения и военной техники: методологические основы. /Монография, под ред. И.Б. Чепкова. – К.: ЦНИИ ВВТ ВС Украины, 2016.

2. Андрушко М.В. Аналіз завдань радіотелеметричних системи при проведенні випробувань озброєння та військової техніки. Системи і технології в'язку, інформації та кібербезпеки: актуальні питання і тенденції розвитку. Збірка тез доповідей на І Міжнародній науково – технічній конференції ВІТІ 26 листопада 2021р. – Київ: ВІТІ, 2021. – с.77-78.

3. Андрушко М.В. Аналіз принципі побудови уніфікованої інформаційно-вимірювальної радіотелеметричної системи для забезпечення проведення випробувань озброєння та військової техніки. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності. Збірка тез доповідей на науково–практичній конференції НАСВ 18 листопада 2021р. – Львів: НАСВ, 2021. – с.177.

4.Кузьміч О.Є. Розгляд алгоритмів вибору та формуванняскладовихбортовихінформаційно-вимірювальнихкомплексівтареєструючих систем. Особливості їх застосування / О.Є.Кузьміч, П.Л.Аркушенко, М.В. Андрушко, І.Г.Гайдак, С.В.Пащенко // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. – Чернігів: ДНДІ ВС ОВТ, 2021. – Вип. № 3(9). – С.73-78.

Артюх С.Г. (ВІТІ ім. Героїв Крут)
д.т.н. Жук О.В. (ВІТІ ім. Героїв Крут)
д.т.н. Романюк В.А. (ВІТІ ім. Героїв Крут)
к.т.н. Степаненко Є.О. (КВЗ КБ)

АНАЛІЗ ЗАГРОЗ ТА АТАК В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність. На даний час в процесі ведення бойових дій для збору інформації та розвідданих провідними арміями країн НАТО активно використовуються безпроводові сенсорні вузли та мережі. Одним із завдань управління безпроводовими сенсорними мережами (БСМ) є забезпечення їх безпеки [1].

Постановка задачі. Провести аналіз існуючих загроз, вразливостей та потенційних атак на БСМ, надати рекомендації з побудови архітектури системи виявлення атак.

Основні положення. Атакою на інформаційну систему називається дія або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загрози шляхом використання вразливостей цієї інформаційної системи. Класифікація загроз наведена
на рис. 1.

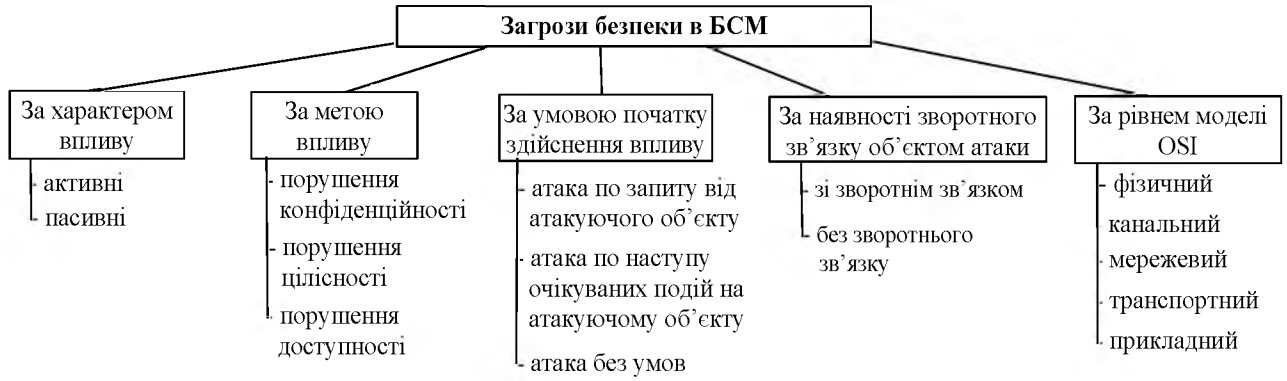


Рис. 1. Класифікація загроз в БСМ

Вразливості БСМ у порівнянні зі стаціонарними мережами та мережами MANET визначаються особливостями їх архітектури та протоколів функціонування [2]:

– обмеженість фізичної безпеки радіоканалу. Широкомовна природа радіоканалу дозволяє супротивникові ставити активні й пасивні завади, здійснювати перехоплення та аналіз мережевого трафіку і розкривати існуючу систему управління сенсорною мережею;

– вузол може бути захоплений на полі бою супротивником або скомпрометований;

– топологія й колективна робота вузлів припускають вразливість функціонування протоколів канального, мережного та інших рівнів;

– обмеженість ресурсів сенсорних вузлів: ємність батареї, обсяг пам'яті, продуктивність процесора вузла; пропускна здатність радіоканалу й ін.

За аналогією із проводовими мережами та мережами MANET атаки в БСМ залежно від характеру дій супротивника діляться на активні й пасивні (рис. 2). Пасивні атаки здійснюються шляхом несанкціонованого прослуховування радіоефіру та аналізу мережевого трафіка. У цьому випадку атакуюча сторона не порушує нормальну роботу протоколів інформаційного обміну.

Пасивні атаки відбуваються без впливу на процес передачі інформації, у той час як активні атаки включають перетворення, модифікацію і/або введення помилкової інформації (у тому числі й керуючої). Результат дій активних атак може варіюватися від блокування окремих вузлів, зниження продуктивності мережі (або її ділянки) до повної дезорганізації її роботи. Головна відмінність активних атак від пасивних полягає в тому, що вони можуть бути виявлені. У свою чергу активні атаки діляться: на зовнішні (супротивник використовує

власне устаткування, відсутність скомпрометованих вузлів) і внутрішні (наявність у мережі скомпрометованих або захоплених вузлів мережі) [3].

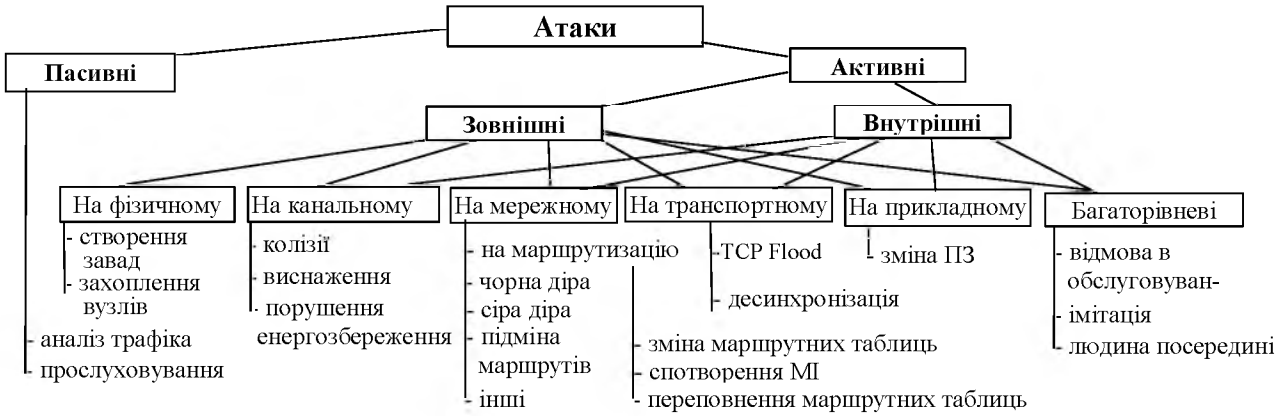


Рис. 2. Класифікація атак в БСМ

Захист від зовнішніх атак включає застосування криптографічних методів: шифрування інформації, використання цифрового підпису. Так цифровий підпис дозволяє перевірити дійсність, цілісність повідомлення, а також забезпечити його неспростовність (забезпечує захист від атак типу відмова, підміна та модифікація переданих даних). Для виявлення дублікатів пакетів і дотримання необхідного порядку їхнього надходження доцільно використовувати у форматі пакета тимчасові мітки й порядковий номер пакета. Однак, криптографічні методи не можуть забезпечити захист від впливу супротивника при наявності скомпрометованих або захоплених вузлів. Для захисту від внутрішніх атак передбачається використовувати системи виявлення атак (СВА) або Intrusion Detection System (IDS).

Висновки. Проведений аналіз існуючих загроз, вразливостей та потенційних атак на БСМ дозволяє зробити висновок, що захист у БСМ від зовнішніх атак повинен здійснюватися методами криптографічного захисту ,а від внутрішніх атак – застосуванням систем виявлення атак.

Проведений аналіз варіантів побудови СВА дозволяє зробити наступні рекомендації з їхньої побудови:

− архітектура конкретної СВА буде визначатися архітектурою БСМ (для ієрархічних БСМ військового призначення доцільна архітектура "агент-менеджер");

− кожен вузол мережі повинен бути оснащений децентралізованою локальною СВА реального часу з можливістю колективного прийняття рішень по виявленню атак і відповідній реакції;

− перспективною технологією прийняття рішень у СВА є інтелектуальні мобільні агенти з використанням нейронних мереж і/або нечіткої логіки;

– функціонування СВА вузла повинне бути погоджене по рівнях еталонної моделі взаємодії відкритих систем і функціях системи управління БСМ військового призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жук О.В., Романюк В.А., Бовда Е.М. Управління перспективними неоднорідними безпровідними сенсорними мережами тактичної ланки управління військами: проблема і шляхи рішення. *Збірник наукових праць "Труди університету"*. №1 (140). 2017. С. 171–180.

2. Жук О.В., Романюк В.А., Остапенко О.О. Аналіз методів та протоколів управління тактичними сенсорними мережами на різних рівнях моделі OSI. *Збірник наукових праць "Труди університету"*. 2016. №2 (135). С. 204–214.

3. S. Shanthi and E. G. Rajan, "Comprehensive Analysis of Security Attacks and Intrusion Detection System in Wireless Sensor Networks," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, pp. 426-431, 2016.

Ph.D Бабарика А.О. (НАДПСУ)
Городиський Р.О. (НАДПСУ)

АКТУАЛЬНІ ПРОБЛЕМИ ДОСЛІДЖЕННЯ МЕТОДІВ СУПРОВОДЖЕННЯ ОБ'ЄКТІВ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

На сьогоднішній день, методи виявлення та супроводження об'єктів на відеопослідовностях активно використовуються в різноманітних областях людської діяльності: контроль якості продукції, медицина, робототехніка тощо. В сучасних системах відеоспостереження з функціями автоматизованої обробки відеоінформації однією з важливих задач є виявлення рухомих об'єктів та побудова траєкторій їх руху.

Виходячи з визначених задач, актуальним завданням є проведення дослідження методів виявлення та супроводження траєкторії рухомих об'єктів в секторах огляду камер відеоспостереження.

Під поняттям виявлення об'єкта будемо розуміти процес визначення місця розташування об'єкта у кадрі. Під поняттям супроводження виявлених об'єктів – процес локалізації рухомого об'єкта чи кількох рухомих об'єктів на послідовності фреймів.

На методи супроводження накладаються різноманітні вимоги, такі як необхідність працювати в режимі реального часу, використання при умові наявності завад, змін фону, контрастності та неоднорідності самого об'єкта супроводження.

Робота методів супроводження виявлених об'єктів, зазвичай, поділяється на наступні етапи:

1. Етап виявлення, під час якого працює алгоритм виявлення нових об'єктів та об'єктів, які були «загублені» алгоритмом супроводження під час роботи другого етапу.

2. Етап супроводження розпочинається тоді, коли припиняється етап виявлення. На цьому етапі алгоритм відслідковує об'єкт при його переміщенні у кадрі за допомогою створеного об'єктного трекера.

Для реалізації першого етапу широкого поширення отримали такі методи як алгоритм Віоли-Джонса, HOG, DPM, RCNN, SPPNet, Fast RCNN, Faster RCNN, FPN, YOLO, SSD, RetinaNet тощо.

Алгоритми супроводження, на відміну від алгоритмів виявлення здатні вирішити задачі при таких несприятливих умовах як оклюзія (об'єкт частково або повністю перекритий), розмиття у русі, складний фон, зміни освітлення тощо.

Існуючі методи супроводження виявлених об'єктів поділяються на наступні категорії: методи основані на супроводженні за «контрольними» точками, методи основані на супроводженні за центрами мас об'єктів (ядром), методи основані на супроводженні за контурами об'єктів.

Широке розповсюдження отримали нейромережеві методи супроводження. Зазвичай, зображення можуть мати достатньо велику кількість змінних, що ускладнює їх обробку детерміністськими методами. Саме тому простір можливих варіацій параметрів об'єктів відносно швидко обробляється нейромережевими алгоритмами. Але нейронні мережі мають і недоліки: алгоритм може показувати гарні результати на навчальній вибірці, але на прикладах, які не приймали участі в навчанні, система може показати гірші результати.

Враховуючи що алгоритми супроводження вирішують дві задачі: виявлення та супроводження, відповідно кожен з етапів необхідно досліджувати та оцінювати за різними показниками, актуальною задачею є продовження досліджень за напрямками: аналіз методів виявлення об'єктів та аналіз методів супроводження виявлених об'єктів.

Балан А.В. (ВІТІ ім. Героїв Крут)
Толстих В.А. (ВІТІ ім. Героїв Крут)
Наконечний Д.О. (ВІТІ ім. Героїв Крут)

АНАЛІЗ СПОСОБІВ ЗАШУМЛЕННЯ МОВНОГО СИГНАЛУ

Актуальність. При проведенні переговорів дорогі та складні попередні перевірки приміщень на наявність підслуховуючої апаратури та технічних каналів витоку інформації можуть виявитися марними, оскільки не виключено, що апаратура, що підслуховує, може потрапити до приміщення напередодні проведення конфіденційних (таємних) переговорів або буде внесена безпосередньо учасниками цих переговорів. Існує різноманітна апаратура для оперативного контролю службою безпеки учасників переговорів. Крім того, треба враховувати, що техніку можуть пронести у вимкненому стані.

Слід також брати до уваги наявність віброакустичних каналів витоку мовної інформації та погану звукоізоляцію приміщень для зчитування конфіденційної інформації можуть використовуватися не тільки апаратні канали витоку мовної інформації, але й природні, такі як повітря, несучі конструкції, труби опалення, водопроводу, вентиляційні канали і т.д..

Постановка задачі. Завдання захисту від витоку полягає у перекритті всіх можливих каналів та нейтралізації засобів перехоплення (мікрофони, спрямовані мікрофони, диктофони, стетоскопи, заставні пристрої, лазерні чи інфрачервоні системи тощо).

Найбільш надійним напрямом протидії несанкціонованому отриманню мовної інформації є перешкоджання звукозапису переговорів або її ретрансляції з приміщення шляхом створення шумової акустичної перешкоди, що забезпечує приховування інформативного сигналу, при цьому співвідношення величина шумового сигналу / величина інформативного сигналу повинно забезпечувати надійне приховування інформативного сигналу меж.

Існуючі засоби захисту акустичної інформації вібраційними каналами являють собою генератори шуму (білого або забарвленого) мовного діапазону частот у комплекті з п'єзоелектричними або електромагнітними віброперетворювачами. Основне призначення їх створення шумових перешкод засобам знімання інформації в стінах, вікнах, інженерних комунікаціях. Основний критерій забезпечення захисту - перевищення шуму над рівнем наведеного в ці конструкції інформативного сигналу. Норми перевищення визначено відповідними нормативно-технічними документами.

Насамперед декілька визначень:

- **«білий» шум** – має рівномірний спектр у смузі частот мовного сигналу;
- **«забарвлений» шум** - формується з «білого» відповідно до огинаючого амплітудного спектру мовного сигналу, що приховується;
- **«мовоподібні» перешкоди** – формуються шляхом міксування в різних поєднаннях відрізків мовних сигналів і музичних фрагментів, а також шумових перешкод, або формується з фрагментів мовного сигналу, що приховується, при багаторазовому накладенні з різними рівнями.

Для формування «забарвленого» шуму, одержуваного з «білого» відповідно до огинаючого амплітудного спектру мовного сигналу, що приховується, в п'яти октавних смугах діапазону 100 - 6000 Гц проводиться оцінка параметрів мовного сигналу і здійснюється коригування рівня шуму в тих же смугах за допомогою вбудованих еквалайзерів. Таким чином, забезпечується енергетична оптимальність перешкоди, при якій задане нормоване співвідношення «сигнал/перешкода» витримується в межах всього діапазону частот мовного сигналу, що захищається.

У більшості робіт, що висвітлюють активні методи захисту мовної інформації – маскування мовного сигналу перешкодою, – особливе місце займають методи, в яких використовується так звана «мовоподібна» перешкода (далі - МПП), що забезпечує високу

ефективність захисту у поєднанні з достатнім рівнем комфортності сторін, що беруть участь у мовних переговорах.

Основні положення. У більшості публікацій, що стосуються різних аспектів застосування МПП, розглядаються методи їх генерації, способи застосування «мовоподібних» перешкод у конкретних (типових) умовах, оцінюються рівні перешкод, що гарантують надійний захист мовного сигналу і т. д.. Ці відомості отримані в ході проведення серій окремих досліджень, що виконуються, як правило, індивідуально, поза рамками будь-якої загальної системної методології, тому наведені результати в цілому носять фрагментарний, уривчастий характер, залишаючи нез'ясованими низку аспектів, зокрема:

Чи загальне визначення МПП?

Фахівцями пропонуються різні визначення поняття МПП залежно від варіанта формування цієї перешкоди. Так, наприклад, деякі дослідники описують МПП як перешкоду, сформовану шляхом міксування в різних поєднаннях відрізків мовних сигналів, музичних фрагментів і шумових перешкод, або сформовану з фрагментів мовного сигналу, що приховується, при його багаторазовому накладенні з різними рівнями, або шум з огинає амплітудного спектру, подібної огинає спектра мовного сигналу, що захищається.

Надійними шляхом зашумлення мовного сигналу є генерація перешкод з «зворотним зв'язком» – адаптивних перешкод. Суть цього методу генерації полягає в аналізі корисного звукового сигналу в приміщенні за допомогою вбудованого мікрофона, після чого генератор автоматично встановлює рівень шуму на тих чи інших частотах, що дозволяє знизити негативні моменти роботи людей в виділеному зашумленому приміщенні.

Найбільш ефективним вважається **адаптивний «мовоподібний» шум**. Він створюється прямо з розмови, що захищається шляхом багаторазового накладання його фрагментів один на одного з різними рівнями інтенсивності сигналу. Перші ж звуки, сказані учасниками конфіденційних переговорів, уловлюються генератором і вирушають до блоку перетворення. Там вони піддаються обробці, в процесі якої відбувається множення та розподіл їх частотних складових. Перешкода, що вийшла в результаті цього процесу, випромінюється колонками. Шум поєднується з інформативним смисловим сигналом, відбивається від стін, стелі та предметів інтер'єру і через якийсь проміжок часу знову вловлюється мікрофоном. Таким чином, виходить безперервний процес генерації дуже ефективного шумоподібного шуму. Крім високої надійності такий генератор має ще один плюс – він працює лише тоді, коли ведеться розмова (коли у приміщенні тихо – шуми не створюються).

З огляду матеріалів, що з питаннями генерації та застосування МПП, можна дійти невтішного висновку, що тепер основний підхід до визначення поняття «мовоподібна» перешкода – описово-технологічний, який спирається фіксацію способу формування та застосування МПП у кожному конкретному випадку.

Висновок. За результатами розгляду та аналізу ряду робіт, що описують різні способи зашумлення акустичної інформації, виходячи з умови, що поставлене завдання захисту мовної інформації – не дати зловмиснику можливість розібратися в смисловому наповненні переданого мовного повідомлення, найбільш перспективним способом захисту мовної інформації є використання мовної перешкоди (МПП)). При цьому враховується, що МПП дає можливість не просто замаскувати інформацію, а й суттєво спотворити зміст сприйманого зловмисником повідомлення.

Що ж до способу оцінювання ефективності застосування МПП, то найбільш об'єктивним та результативним джерелом відомостей для вирішення цього завдання є проведення артикуляційних випробувань. Зокрема, при виконанні низки вимог до складання таблиць артикуляції та методу обробки отриманих результатів, артикуляційні випробування дозволяють вийти за рамки суто формального структурно-синтаксичного оцінювання якості прийому мовного сигналу, створюючи умови та можливості для оцінювання рівня семантичної близькості прийнятого аудитором повідомлення переданої вихідної (незашумленої) мовної інформації.

Безносенко С.Ю. (ВІТІ ім. Героїв Крут)
Коротченко Л.А. (ВІТІ ім. Героїв Крут)
Савіцький Л.М. (ВІТІ ім. Героїв Крут)
Глобін А.В. (ВІТІ ім. Героїв Крут)

ПРІОРИТЕТНІ НАПРЯМКИ РОЗВИТКУ КОМБІНОВАНИХ ЦИФРОВИХ РАДІОСИСТЕМ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ НВЧ ДІАПАЗОНУ

На сьогоднішній день є актуальна задача створення сучасної мобільної комбінованої станції цифрового тропосферного і супутникового зв'язку НВЧ діапазону, яка одночасно працює в 2-х режимах: загоризонтного зв'язку і прямої видимості. Під час розгляду даної проблеми проведено розгляд сучасного стану тропосферного зв'язку у світі. Технічні характеристики передових розробок цифрових тропосферних станцій та систем управління зарубіжних компаній Comtech Systems, Корпорація Raytheon, General Dynamics, Advantech Wireless показали, що тропосферні модеми різних виробників мають пропускну спроможність на рівні від 50 Мбіт/с до 150 Мбіт/с, які забезпечують стійкий багатопроменевий зв'язок з прямим виправленням помилок (FEC) та забезпечує роботу з портами даних такими як Gigabit Ethernet (GbE) і протоколом SNMP, який є ключовим елементом для створення новітньої мобільної комбінованої станції цифрового тропосферного і супутникового зв'язку.

Аналіз стану розвитку сучасного тропосферного зв'язку у світі показав, що одним з провідних світових лідерів в області тропосферного зв'язку є американська компанія Comtech Systems, цифрові тропосферні системи якої розгорнуті у всьому світі.

Основними перевагами розробки компанії Comtech Systems є:

1) цифровий модем для тропосферного зв'язку CS67200, який містить такі функції, як пряме виправлення помилок (Comtech's Turbo Product Code Forward Error Correction), автоматичну підтримку швидкості передачі (Automatic Code Rate) і автоматичне регулювання потужності (Automatic Power Control), які дуже широко використовують в сучасних систем заобрійного зв'язку, як для комерційних, так і для оборонних завдань;

2) частотний конвертер CS4400, призначений для роботи на тропосферних лініях, так і на лініях прямої видимості, на частотах 4,4–5 ГГц який застосовується в тропосферних системах по всьому світу;

3) цифровий мультиплексор CSM8100 (8E1/IP) є першим в світі мультиплексором, що одночасно підтримує, як протоколи систем SDH, так і протоколи пакетних систем;

4) твердотільні підсилювачі потужності TRP500-4450 ($P_{вих}$=500 Вт) і CS42000 ($P_{вих}$ = 2000 Вт) для систем тропосферного зв'язку, які підходять як для внутрішнього, так і зовнішнього застосування;

5) Transportable Fast Link Antenna (TFLA) — це переносна трьохметрова тропосферна антена з кутовим рознесенням (антенний пост), яка розгортається за 30 хвилин двома операторами та підтримує функцію автоматичного наведення на кореспондента і може експлуатуватися при швидкості вітру до 30 м/с. Система управління цих цифрових тропосферних станцій оснащені виносними і стаціонарними пультами управління з підтримкою декількох протоколів і з можливістю програмної переконфігурації кінцевих пристроїв.

Таким чином, перспективність створення комбінованих цифрових радіосистем НВЧ діапазону, що відповідають тенденціям розвитку тропосферних і радіорелейних засобів зв'язку є актуальним напрямком для розробки комбінованих цифрових телекомунікаційних систем з використанням терагерцового діапазону для суттєвого підвищення пропускної здатності та завадозахищеності і скритності радіоліній зв'язку.

Березовський Д.В. (ВІТІ ім.Героїв Крут)
Світайло К.В. (ВІТІ ім.Героїв Крут)

БАГАТОАНТЕННІ ТЕХНОГОЛОГІЇ В СИСТЕМАХ РАДІОЗВ'ЯЗКУ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ.

Одним з новітніх зразків озброєння на полі бою стали безпілотні авіаційні комплекси, які під час воєнних конфліктів довели свою здатність значно ефективніше, ніж пілотовані літаки, вести повітряну розвідку та виконувати інші завдання бойового забезпечення, а також для завдання ударів по противнику.

На сьогоднішній день використання безпілотних літальних апаратів (БЛА) у військовій сфері набуло великих оборотів, тому дуже велика увага приділяється розробці перспективних безпілотних авіаційних комплексів, що складаються із двох основних елементів:БЛА і наземного пункту управління.

Одна з найбільш актуальних проблем у сучасних системах зв'язку – необхідність підвищення пропускної спроможності та швидкості передачі даних, а також збільшенні кількості абонентів. Але зі збільшенням швидкості - втрачаємо якість передачі. Тому дане питання єактуальним на сьогоднішній день.

У зв'язку із вимоги до біологічної та електромагнітної сумісності накладаються обмеження на підвищення випромінюваної потужності та розширення смуги частот. За таких обмежень проблема недостачі пропускної спроможності та швидкості передачі даних змушує шукати нові ефективні методи її вирішення. Одним із найефективніших методів – застосування адаптивних антенних решітки зі слабо корельованими антенними елементами.

Метою даної роботи є підвищення ефективності наземного управління БЛА за рахунок модернізації його комплексу антенно-фідерних пристроїв.

На цьому принципі заснована технологіяMIMO (Multiple Input Multiple Output) - це роздача відразу кількох потоків інформації по одному каналу з наступним проходженням їх через пару або більше антен до попадання в приймальні незалежні пристрої для трансляції радіохвиль. Це дозволяє суттєво покращити пропускну здатність сигналу, не вдаючись до розширення смуги.

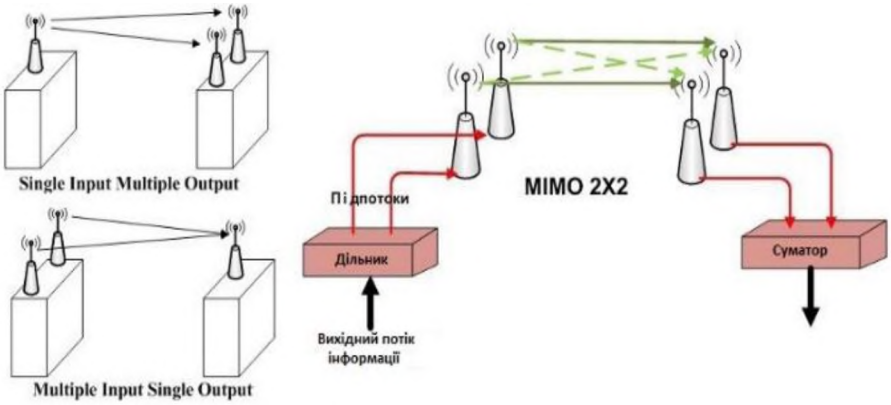


Рис.1. Приклад системи MIMO

Як бачимо, MIMO дає шанси збільшити швидкість трансляції сигналу більш ніж двічі. Досягається це завдяки монтажу в коробі відразу кількох антен, які мають у своєму розпорядженні на незначному видаленні одна від одної. Одночасне отримання, а також роздача цифрового потоку антенами до одержувача відбувається через два незалежні кабелі. Це дозволяє суттєво збільшити швидкісні параметри.

Зазвичай у 4G число каналів MIMO кратне двом - 2, 4, 8 (у Wi-Fi системах набула поширення трьохканальна система 3x3) і рекомендується, щоб їхнє число збігалося і на базі і на модемі. Тому для фіксації цього факту MIMO визначають з каналами прийом передачі - 2×2 MIMO, 4×4 MIMOі т.д. Поки що в наш час ми маємо справу переважно з 2x2 MIMO.

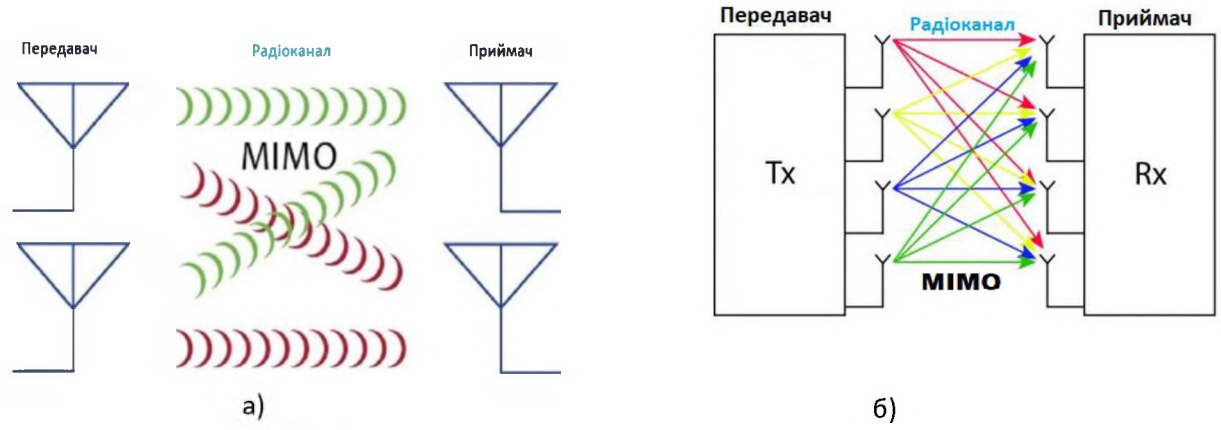


Рис.2.Види систем MIMO: а)2×2 MIMO, б)4×4 MIMO.

Які антени застосовуються у технології MIMO? Це звичайні будь-які антени, просто їх має бути дві (для 2×2 MMO). Для поділу каналів застосовується ортогональна, так звана X-поляризація. При цьому поляризація кожної антени щодо вертикалі зрушена на 45 °, а щодо один одного - 90 °. Такий кут поляризації ставить обидва канали в рівні умови, оскільки при горизонтально/вертикальній орієнтації антен один з каналів неминуче отримав би більше загасання через вплив земної поверхні.

На рисунках зображені приклади компоновки антен в системі MIMO:

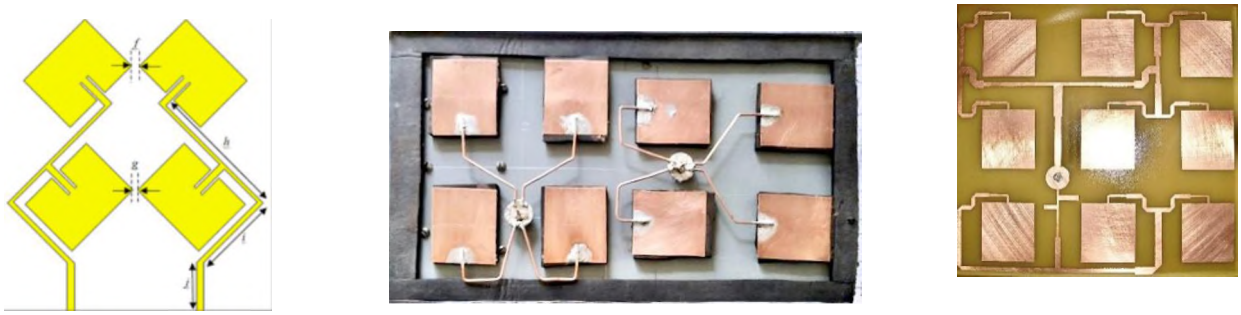


Рис.2. Компоновка антен системи MIMO: а) 4×4 MIMO, б) 8×8 MIMO, в) 9×9 MIMO.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Банков С.Е. Антени супутникової навігації: аналіз характеристик низькопрофільних антен / Збірник наукових праць. Видавництво «Перо», 2014р. стор. 154–172.

2.М. Дженсен М. Райс, Т. Нельсон, А. Андерсон.Ортогональна подвійна антена для рознесення передачі для SOQPSKв каналах аеронавігаційної телеметрії. – Збірник працьМіжнродна телеметрична конференція, Сан-Дієго,С.А, жовтень 2004 р., стор. 337–344.

3. Ілюшко В.М., Наритник Т.М. Система передачі даних на базі висотного безпілотного літального апарату(СПД "Фаєтон"). – Зв'язок, 2004, №7, с. 38–45.

Болотюк Ю.В. (ВІТІ ім. Героїв Крут)

ОСОБЛИВОСТІ РОЗРАХУНКУ ПОКАЗНИКІВ НАДІЙНОСТІ КАНАЛУ ПЕРЕДАЧІ ДАНИХ

Вирішення завдань технічного діагностування для систем з вбудованим програмним забезпеченням вимагає пошуку відповідних моделей поведінки подібних систем. В низці робіт присутні моделі зміни діагностичного параметру під час старіння елементної бази обчислювальних засобів та зміни показників надійності програмного забезпечення під час функціонування. Однак, слід зазначити, що до складу функціонуючих систем з вбудованим програмним забезпеченням входить ще один компонент – середовище передачі даних, що з'єднує окремі територіально рознесені комплекти системи. В роботі не розглядається радіоканал, у зв'язку з тим, що властивості цього середовища мають дуже змінний характер навіть протягом одного сеансу обміну даним. Також за межі дослідження винесено проводові лінії зв'язку, оскільки параметри цього середовища майже не змінюються протягом усього часу функціонування. Метою дослідження є волоконно-оптичні лінії зв'язку(ВОЛЗ), та динаміка (модель) поведінки цієї складової систем з вбудованим програмним забезпеченням.

Аналіз основних технічних вимог, параметрів і умов застосування оптоволокна (ОВ) показав, щотеоретичні властивості матеріалу ОВ значно відрізняються від отриманих на практиці. Тому при проведенні технічного діагностування систем з вбудованим програмним забезпеченням слід звертати увагу на середовище передачі даних та його характеристики.

У ВОЛЗ має місце нове порівняно з традиційними кабельними лініями зв'язку внутрішнє джерело відмов – обриви ОВ, викликані старінням кварцового скла.Під старінням розуміється зміна частоти кристалу кварцу з плином часу, що призводить до поступової незворотної зміна передавальних і механічних характеристик оптичного кабелю.Коли ці зміни перевищать допустимі норми, кабель частково або повністю вийде з ладу.

До проблем, які виникаютьпід час експлуатації ОВ відносяться: зниження напруги в монтажній структурі кристала, внутрішнє забруднення, поглинання вологи і зміни в самому кварці. Старіння кварцового скла призводить до зміни частоти, що може мати вирішальне значення при проектуванні телекомунікаційних мереж. На старіння в кристалах кварцу впливають два основних фактори: масообмін і напруга.Результати проведених тестів на старіння кварцових кристалів показують, що зміна частоти, як правило, найбільша протягом першого року і з часом зменшується. Характеристики старіння кристалів відбуваються за логарифмічною кривою.

Зміна властивостей оптоволокна, як сукупності кварцових кристалів, визначається через відносну кількість кристалів, які «зістарілися». Кількість цих кристалів вимірюється в *ppm*(одиниця вимірювання концентрації)(англ. Partspermillion, «частин на мільйон»).

Тестова перевірка показала, що зміна властивостей кварцового скла становить на рівні ±5*ppm* на рік (за 5 років становитиме ±25*ppm*). При цьому, відхилення в межах від ±1*ppm* до ±2*ppm*відбуваються протягом першого року експлуатації, а потім зменшується протягом наступних років. «Керівним правилом» є старіння кристалів ±10*ppmmax* протягом 10 років, хоча кристал розпадається зазвичай набагато менше в реальності.Це визначає особливості розрахунку показників надійності ВОЛЗ.

Старіння кварцового волокна призводить до втрат потужності переданого сигналу і вимірюється в дБ/км. Величина 3 дБ означає, що половина потужності втрачена. Втрата 10 дБ означає, що тільки 1/10 потужності джерела доходить до приймача, втрати 90%.

ВОЛЗ, як правило, здатні нормально функціонувати при втратах в 30 дБ (прийом всього 1/1000 потужності). Розрізняють два види втрат:

- втрати на поглинання – пов'язані з перетворенням одного виду енергії в інший. Електромагнітна хвиля певної довжини викликає в деяких хімічних елементах зміну орбіт електронів, що, в свою чергу, веде до нагрівання волокна. Природно, що процес поглинання хвилі тим менше, чим менше її довжина, і чим чистіше матеріал волокна;

- втрати на розсіювання – зниження потужності сигналу означає вихід частини світлового потоку з хвилеводу. Обумовлено це зазвичай неоднорідностями показника заломлення матеріалів. Відомо, що зі зменшенням довжини хвилі втрати розсіювання зростають.

Значний вплив на процес старіння кварцового скла становить корозія ОВ, під якою розуміється руйнування ОВ при дії на нього механічної напруги та вологи. Коефіцієнт інтенсивності напруги визначається як МПа·м1/2.

Наявність мікротріщин або дефектів на поверхні ОВЛЗ служать джерелами руйнування при напругах набагато нижче теоретично допустимих. Мікротріщина утворюється в два етапи. У першому етапі $K_1<K_{1кр}$, де $K_{1кр}$ — критичне значення коефіцієнта інтенсивності напруг. Для кварцових оптичних волокон $K_{1кр}$=0,789 МПа·м1/2. На цьому етапі відбувається безперервне зростання мікротріщини відповідно до диференціального рівняння $dc/dt = AK_1n$, де *A*-постійна, яка залежить від матеріалу ОВ; *n* - постійна, яка залежить як від матеріалу ОВ, так і від зовнішніх умов (коефіцієнт корозії). На другому етапі $K_1=K_{1кр}$ і зростання мікротріщини до повного розсічення волокна відбувається практично миттєво (частки секунди).

Оптичні волокна можуть мати велику кількість мікротріщин, спричинених технологічними причинами. Для визначення міцності ОВ залежно від прикладених навантажень використовують функцію кумулятивної небезпеки обриву, яка є залежністю числа обривів на метр від величини прикладених навантажень.

Оцінюючи термін служби ВОЛЗ слід враховувати можливість значного збільшення згасання після відновлення зв'язку.Кількісно надійність ВОЛЗ може бути виражена ймовірністю безвідмовної роботи, яка визначається за формулою:

$$P(t,L) = \exp\left[-\int_0^T (\sum_{i=1}^{n} \overline{\Lambda_i}(t) L_i) dt\right]$$

де L_i –довжина і-тої ділянки (вважається, що ВОЛЗ складається з декількох ділянок з однаковими умовами експлуатації); Т –проміжок часу, для якого визначається ймовірність безвідмовної роботи; Λ_i –інтенсивність відмов для *i*-тої ділянки.

Інтенсивність відмов за певний проміжок часу представляється сумою складових, обумовлених відмовами через зовнішні фактори впливу $\Lambda_{вн}$, відмови муфт і зростків ОВ $\Lambda_м$ та обривами ОВ через старіння скла $\Lambda_{ст}$. Величини $\Lambda_{вн}$ і $\Lambda_м$ визначаються з досвіду експлуатації ліній зв'язку:

$$\overline{\Lambda}(t) = \overline{\Lambda_{вн}} + \overline{\Lambda_м} + \overline{\Lambda_{ст}}(t).$$

Однією з основних проблем довговічності ВОЛЗ являється інтенсивність старіння елементної бузи каналу передачі (оптичного волокні і з'єднувальних муфт), так як від цього залежить кількість відмов на лінії.

Аналіз надійності ВОЛЗ необхідно проводити, як у процесі розробки і виготовлення, так і у процесі проектування, будівництва та експлуатації кабельних ліній.

У якості діагностичного параметру для розв'язання задач технічної діагностикив роботі обрано енерго-часовий діагностичний параметр. Відповідно до назви, в ньому об'єднано зміни енергетичної складової в системі при обміні спеціальними перевірними тестовим послідовностями, та зміни часової складової (в тому числізміни частоти).

Оцінюючи процеси старіння оптоволоконних ліній маємо зміни і одної і другої складової в тестовому сигналі.

Задача контролю технічного стану телекомунікаційної мережі на основі оптоволоконних ліній покладається на автономну автоматизовану систему діагностування, оскільки проведення процедур діагностування без засобів автоматизації в сучасних умовах практично не можливо.

Бондаренко Л.О. (ВІТІ ім. Героїв Крут)
Бондаренко О.Є.(ВІТІ ім. Героїв Крут)
Яковчук О.В. (ВІТІ ім. Героїв Крут)
Макарчук В.І. (ВІТІ ім. Героїв Крут)

ПІДХІД ДО ОЦІНКИ ЯКОСТІ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ

При здійсненні управлінських функцій посадовими особами органів військового управління проявляється складне поєднання військових, соціальних, організаційно-технічних та інших аспектів діяльності. Їх вивчення і дослідження вимагають застосування різноманітних методів: спостереження, порівняння, аналізу, синтезу, аналогій, фізико-математичного моделювання з використанням сучасних засобів автоматизації.

Особливе значення в удосконаленні методів вивчення систем управління (СУ) угруповань військ (сил) має системний підхід, який дозволяє проводити аналіз всіх істотних сторін і аспектів управління в їх взаємозв'язку і взаємозалежності, а також розглядати їх в єдиній системі.

Що стосується СУ угруповань військ (сил), то системний підхід передбачає оцінку основних її складових компонентів (командування, штаб, система зв'язку і т. п.) в комплексі, тобто з урахуванням найбільш показових властивостей кожного компонента і з урахуванням їх ієрархічного і взаємопов'язаного функціонування.

Під частковим показником якості системи розуміється ступінь реалізації нею деяких вимог, що визначають функціонування системи, у конкретних умовах обстановки. Наприклад, частковий показник якості управління «прихованість» характеризує ступінь виконання вимоги до системи управління зберігати потай від противника елементи СУ і інформацію, що циркулює в ній.

Органами військового управління військовими формуваннями (ОВУ) є пункти управління (ПУ), які об'єднані в ієрархічну схему з прямими (командними) та рокадними (взаємодіючими) зв'язками різного ступеня важливості.

У цьому випадку потенційними бойовими можливостями СУ буде загальна кількість ПУ у контурі управління - Органами військового управління військовими формуваннями (ОВУ) є пункти управління (ПУ), які об'єднані в ієрархічну схему з прямими (командними) та рокадними (взаємодіючими) зв'язками різного ступеня важливості.

У цьому випадку потенційними бойовими можливостями СУ буде загальна кількість ПУ у контурі управління – N.

Реалізація ж потенційних бойових можливостей при такому підході оцінюється величиною, що характеризує середню кількість підлеглих ПУ, які керуються з необхідною якістю – M.

Тоді ступінь реалізації бойових можливостей буде відносним числом ПУ, керованих з необхідною якістю, яка і є узагальненою оцінкою якості функціонування ПУ: $k = {}^{M}/_{N}$.

У теоретичних засадах управління розроблено основні вимоги, виконання яких забезпечує необхідну якість процесу управління. До цих вимог відносяться стійкість, безперервність, оперативність і скритність управління. Грунтуючись на цьому, можна запровадити такі приватні показники якості функціонування кожного чинного ПУ:

стійкість – $k_{\text{ст ПУ}}$;

безперервність – $k_{\text{безпер ПУ}}$;

оперативність – $k_{\text{опер ПУ}}$;

скритність – $k_{\text{скр ПУ}}$.

Тоді очевидно, що показники стійкості, безперервності, оперативності та скритності, що розраховуються для всієї системи управління угрупованнями військ (сил) загалом, будуть перебувати у функціональній залежності від тих самих показників, що розраховані для складових сукупності чинних ПУ: $k_{СУ} = F(\ k_{ПУ_1}, k_{ПУ_2} \ \dots \ k_{ПУ_n})$.

де n – кількість діючих ПУ, що входять до системи управління угрупуванням військ (сил).

Якщо ПУ є основними структурними елементами СУ військами (силами), система зв'язку є частиною СУ, яка безпосередньо організує проходження управляючих впливів. Очевидно, що приватні показники якості функціонування ПУ повинні бути у функціональній залежності від приватних показників якості функціонування системи зв'язку.

Щоб виявити цю залежність, необхідно з'ясувати, що являє собою система зв'язку і чим характеризуються її основні елементи.

Система зв'язку створюється задля забезпечення функціонування СУ і є сукупністю взаємопов'язаних і узгоджених по завданням, місцю й часу дій вузлів і ліній зв'язку, що розгортаються за єдиним планом на вирішення завдань забезпечення управління військами чи силами і зброєю. Система зв'язку є найважливішою складовою, матеріально-технічною основою СУ військами (силами) і істотно впливає на бойову ефективність військ.

Для забезпечення потреби СУ в інформаційному обміні та розв'язання завдань управління на базі системи зв'язку створюються інформаційні напрямки, що є сукупністю ліній та вузлів зв'язку, що забезпечують зв'язок між двома пунктами управління.

Очевидно, що інформаційні напрями є тим об'єктом, який пов'язує у єдине ціле всю СУ.

Таким чином, найбільш значущими для оцінки всієї СУ будуть показники якості управління, які розраховані саме для інформаційних напрямів:

стійкість – $k_{ст\ [Н}$;

безперервність – $k_{безпер\ [Н}$;

оперативність – $k_{операН}$;

скритність – $k_{скр\ [Н}$.

Тоді можна зробити висновок, що показники стійкості, безперервності, оперативності та скритності, що розраховуються для ПУ, будуть перебувати у функціональній залежності від тих самих показників, розрахованих для інформаційних напрямів, що пов'язують його з ПУ підпорядкованих (взаємодіючих) військ (сил): $k_{СУ} = F(\ k_{ІН_1}, k_{ІН_2}, \dots \ k_{ІН_m})$,

де m – кількість інформаційних напрямів.

Таким чином, виробляється наступний порядок розрахунку часткових показників якості СУ угрупованнями військ (сил):

- розраховуються часткові показники якості всіх інформаційних напрямів, присутніх у СУ: $k_{ст\ [Н}, k_{безпер\ [Н}, k_{операН}, k_{скр\ [Н}$;

- на основі часткових показників якості інформаційних напрямів, що зв'язують ПУ, розраховуються відповідні часткові показники якості функціонування для всіх ПУ, що діють: $k_{скр\ [Н}, k_{безпер\ ПУ}, k_{опер\ ПУ}, k_{опер\ ПУ}$;

- з приватних показників якості, розрахованих для всіх діючих ПУ, розраховуються відповідні приватні показники якості функціонування всієї системи управління угрупуванням військ (сил): $k_{СУ_{ст}}, k_{СУ_{безпер}}, k_{СУ_{опер}}, k_{СУ_{скр}}$.

Таким чином, розроблений підхід дозволяє отримати значення приватних показників якості СУ угрупованнями військ (сил) відповідно до системного підходу, тобто з урахуванням параметрів основних компонентів та суттєвих аспектів функціонування СУ військами.

Бондаренко Т.В. (ВІТІ ім. Героїв Крут)
Бондаренко Л.О. (ВІТІ ім. Героїв Крут)
Зінченко М.О. (ВІТІ ім. Героїв Крут)
Руденко В.І. (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ МЕТОДІВ МОНІТОРИНГУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Вступ (актуальність або постановка задачі)

Моніторинг телекомунікаційної мережі є невід'ємною частиною системи керування мережею. Системи моніторингу поділяються на типи: централізована та децентралізована (розподілена). Методи моніторингу для кожної мережі індивідуальні та вибираються на основі аналізу характеристик мереж, а також обмежень, що накладаються на систему керування мережею. Класифікація методів моніторингу наведено на рисунку 1.

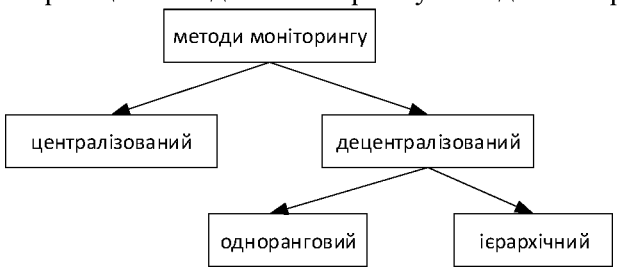


Рис. 1. Класифікація методів моніторингу

Метою дослідження є аналіз методів моніторингу мереж шляхом порівняння їх переваг та недоліків.

Виклад основного матеріалу дослідження

При методі з централізованою архітектурою єдиної системи управління контролюється вся мережа в якій програмно-апаратне рішення системи моніторингу може складатися з одного або кількох серверів. Якщо всі сервери розташовані в одному центрі мережевих операцій (ЦМО), це вважається централізованою архітектурою, де розподілена мережа управляється з центру мережевих операцій. Оператори ЦМО з кожного сегмента використовують клієнтів для віддаленого підключення до серверів централізованого керування, які розташовані в іншому регіоні. Така система має ряд недоліків, основні з яких:

- обмеження можливостей масштабованості системи моніторингу через підвищене завантаження каналів управління та потреби у високій продуктивності менеджера;
- збільшення часу обробки даних моніторингу, що може спричинити втрату актуальності інформації, що в свою чергу, впливає на своєчасність прийняття рішень щодо будь-якого інциденту чи проблеми у керованій мережі;
- відключення системи моніторингу або всієї мережі при збоях у роботі головного менеджера, що призводить до зниження рівня безпеки інформації в мережі, а отже, до загрози втрат її цілісності, доступності та конфіденційності.

Децентралізований метод моніторингу телекомунікаційної мережі дозволяє створювати складні за структурою розподілені системи моніторингу, що дає системі моніторингу більшу стійкість до відмов.

Як правило, розподілена система моніторингу мережі містить велику кількість з'єднань-зав'язків "менеджер-агент", які доповнюються робочими станціями мережевих операторів, коли вони зв'язуються з менеджерами. Кожен агент збирає дані та керує конкретними елементами мережі. Наявність кількох менеджерів дозволяє розподілити навантаження з обробки даних між ними, що забезпечує масштабованість системи та незалежність роботи менеджерів один від одного. Масштабованість системи дозволяє використовувати цей метод у великих мережах.

Два найчастіше підходи, що використовуються – це комбінації відносин менеджер-агент однорангові та ієрархічні. Значно гнучкішим буде ієрархічна побудова зав'язків між менеджерами, як зазначено рисунку 2.

Кожна система управління сегментами мережі встановлюється в ЦМО, який відповідає за моніторинг сегмента/домену, тобто менеджер домену.

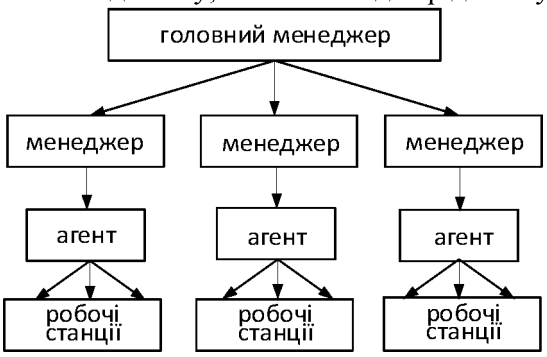


Рис. 2. Схема ієрархічного зв'язку у системі моніторингу

Розробка мережевих моделей моніторингу на різних рівнях проектування необхідно здійснювати за "низхідним" принципом починаючи з верхнього рівня, який визначає склад інформації, яка потрібна від пари "менеджер-агент" нижнього рівня.

При побудові різних систем моніторингу великих мереж зазвичай використовується платформний підхід. Як правило, платформа моніторингу поставляється з якимось універсальним менеджером, який може виконувати деякі основні функції моніторингу без програмування. Базові функції, що включаються до платформи – це мережні зіставлення (група моніторингу конфігурації), функції для відображення стану керованих пристроїв, фільтрація повідомлень про помилки (група моніторингу помилок).

Базові інструменти такої платформи включають функції, необхідні для побудови топології мережі, фільтрації інформації, що передається від агентів до агентів, інструменти підтримки та обробки баз даних. Сукупність інтерфейсних функцій платформи утворює інтерфейс прикладного програмування системи управління, який згодом використовують адміністратори системи або мережі.

На основі цієї схеми можуть бути побудовані системи практично будь-якої складності з великою кількістю агентів та менеджерів різного типу.

Спеціалізоване програмне забезпечення системи моніторингу повинне складатися з трьох окремих програмних компонентів – серверного, клієнтського і агентського програмних модулів, які забезпечують формування інформації для прийняття управлінських рішень.

Розподілений метод мережного моніторингу практично позбавлений недоліків централізованого та може бути реалізований у вигляді ієрархічної структури.

Найбільший інтерес перспективних досліджень представляє принцип побудови систем моніторингу, що засновані на взаємозв'язку методів централізованого та децентралізованого управління, активного і пасивного моніторингу. У цьому випадку проводиться раціональний поділ завдань управління. Саме такий принцип пропонується для застосування в системі автоматизованого управління мережами електронних комунікацій ЗС України.

Висновки.В результаті аналізу методів моніторингу мереж шляхом порівняння їх переваг та недоліків встановлено, що:

централізований метод моніторингу можна використовувати в невеликих мережах;

розподілений метод застосовний до великих мереж;

залежно від масштабу мережі можна використовувати однорангову або ієрархічну архітектуру системи моніторингу;

при побудові різних систем моніторингу великих мереж доцільно використовувати платформний підхід.

Волков А.Ф. (ХНУПС)
Дроздов А.Р. (ХНУПС)

РОЗРОБКА ФОРМАЛІЗОВАНОГО ОПИСУ ПРОЦЕСІВ ПРИЗНАЧЕННЯ ВОГНЕВИХ ЗАСОБІВ НА ПОВІТРЯНІ ЦІЛІ

Процес прийняття рішення на знищення повітряних цілей противника передбачає ретельне оцінювання обстановки, яке включає оцінювання повітряного противника та оцінювання можливостей свого підрозділу. На основі результатів оцінювання противника і можливостей вогневих засобів формулюється рішення щодо застосування вогневих засобів. Процес формулювання такого рішення включає наступні етапи:

– встановлення послідовності знищення засобів противника;

– вибір вогневих засобів для знищення цілей.

Розробка рекомендацій по призначенню вогневих засобів ґрунтується на тих чи інших вихідних положеннях вибору цілей для знищення. Рекомендація містить інформацію про те, який вогневий засіб слід призначити для ураження певної цілі (можуть призначатися й інші вогневі засоби, здатні обстріляти цю ціль).

Найбільш загальними правилами розподілу вогневих засобів є:

– розподіл вогневих засобів з урахуванням важливості цілей для їх точного ураження. Правило вказує на необхідність оцінювання тактичної важливості цілей та вибір найбільш ефективних способів вогневого впливу;

– досягнення максимальної відповідності вогневих засобів характеристикам і параметрам руху цілі, яка була обрана для ураження. Кожна з повітряних цілей, має свої особливості, і відповідно можливості вогневих засобів по ураженню цілей різного типу в різних умовах неоднакові. Виконання даного правила забезпечує найбільшу ефективність вогневих засобів, при цьому по можливості повинні враховуватися швидкості та напрямки польоту цілі, а також тип цілі;

– призначення вогневих засобів для ураження цілей, виходячи з умови мінімального їх входження у зону вогню. Правило означає, що кожна ціль повинна знищуватися відразу ж, як тільки увійде в зону ураження першого вогневого засобу. При цьому максимізується кількість впливів і забезпечується ураження противника на допустимо великих відстанях від об'єкту;

– зосередження вогню по цілях у всіх випадках, коли це можливо. Зосередження вогню забезпечує надійне знищення цілей в умовах радіоелектронного подавлення, їх маневру та ін.;

– призначення кожному вогневому засобу такої кількості цілей, скільки стрільб він може провести в даних умовах обстановки;

– врахування пропозицій нижчого КП при наявності у нього більш повної інформації в даній обстановці. Рішення, яке не відповідає реальній обстановці, не є оптимальним. Тому від наявності та якості інформації в тій чи іншій командній інстанції, залежать ступінь централізації управління вогнем і характер прийнятих рішень.

Кожне з перерахованих вище правил застосовується не ізольовано, а у тісному взаємозв'язку один з одним. При цьому необхідно враховувати стан пунктів управління, вогневих засобів, наявність ракет та ін.

У разі необхідності в ході бою коригуватирішення необхідно уточнити послідовність знищення цілей противника. Пропонується наступний порядок розподілу цілей противника, який може бути змінений експертами:

– в порядку зниження небезпеки цілей;

– в порядку зростання номера категорії цілей;

– першочергові цілі за рішенням відповідного командира.

Гангало І.М.(ДУТ)
д.т.н. Жебка В.В.(ДУТ)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ АЕРОФОТОЗЙОМКИ ДЛЯ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ

Актуальність. Військова розвідка є одним з ключових інструментів успішного проведення військових операцій. Якісно проведена розвідка надає значну перевагу на полі бою і забезпечує інформацією тилові підрозділи для своєчасного реагування на поставлені задачі.

Постановка задачі. Сучасні реалії ведення війни оновлюють вимоги і вимагають вдосконалення способів ведення військової розвідки. Вирішити проблеми безпеки та своєчасного виявлення супротивника покликана повітряна розвідка.

За результатами успішних операцій на Київщині та в інших регіонах України, були отримані певні відомості. Наявність навіть найпростіших цивільних літальних апаратів з камерами для спостереження за місцевістю з повітря, значно збільшувала шанси на виживання, передачу координат, та ураження сил і засобів супротивника.

Мета дослідження. Метою дослідження є аналіз впливу безпілотних літальних апаратів на ведення сучасних бойових дій в рамках виявлення та розпізнавання військової техніки.

Результати дослідження. Безпілотні літальні апарати(БПЛА) значно відрізняються за типами (працюють за принципом літака чи гелікоптера) та параметрами (розмір, дальність польоту, тощо) і їх можна поділити на певні категорії [2]:

- Розвідувальні («Лелека-100», «Фурія», «Валькірія»);
- ударні (сімейство PD першого та другого покоління);
- дрони камікадзе («Switchblade», «RAM II UAV»);
- саморобні ударні (Коптер «Бандерик», переобладнані великі аграрні дрони).

Слід зазначити, що ударні БПЛА можуть виконувати функції розвідки та корегування. Наприклад Bayraktar TB2, який перебував на відстані близько 50 кілометрів від цілі зміг виявити, передати координати та у режимі онлайн корегувати вогонь артилерії по цілям на аеродромі Чорнобаївка [3]. Проте для використання таких складних та вимогливих у експлуатації БПЛА необхідна наземна станція для операторів, спеціально навчений екіпаж та інфраструктура для обслуговування. Цивільні дрони не потребують спеціальної підготовки і можуть використовуватись будь-ким, хто має смартфон. Проте вбудованого функціоналу для того щоб виявити та розпізнати військову техніку, автоматично чи напівавтоматично нанести її на електронну мапу місцевості вони не мають.

Цю проблему можна вирішити використовуючи теорію розпізнавання образів. Маючи набір певних ознак і властивостей можна ідентифікувати об'єкт. Одним із способів реалізації функції розпізнавання об'єктів є поєднання комп'ютерного зору та машинного навчання. Серед найпопулярніших бібліотек для комп'ютерного бачення є OpenCV, SimpleCV, DeepFace, NVIDIA CUDA-X, PyTorch. Кожна з них має безліч користувачів, які готові поділитися готовими рішеннями для пересічних задач. З найпоширеніших розширень для машинного навчання слід виділити Numpy, Scipy, TensorFlow. Саме вибір бібліотек з вільним доступом до коду дає можливість швидко і безпечно модифікувати їх для спеціалізованої галузі, у тому числі військовій розвідці.

OpenCV – бібліотека комп'ютерного зору з відкритим кодом, яка містить в собі функції та алгоритми комп'ютерного зору, обробки зображень, яку використовують у тому числі і розпізнавання об'єктів на фотографіях [1].

TensorFlow – бібліотека з відкритим кодом, яка призначена для побудови та тренування нейронних мереж для виявлення та ідентифікації образів максимально схожим принципом, що і людина [5].

Використовуючи бібліотеки OpenCV та TensorFlow можна утворити модуль, який дає змогу в режимі реального часу ідентифікувати об'єкти та передавати їх місцезнаходження.

Загальну схему роботи модуля можна зобразити на схемі (рис.1).

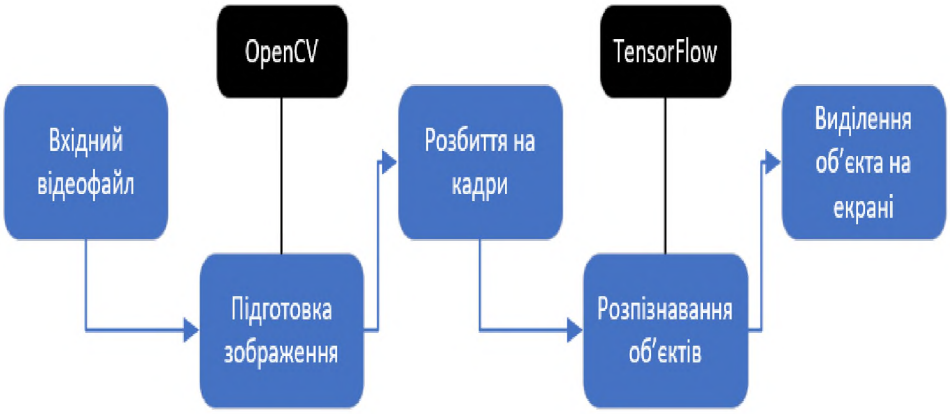


Рисунок 1 – Схема роботи модуля виявлення та розпізнавання об'єкту

Для використання нейронної мережі її потрібно навчити або використати вже готовий набір даних, але при цьому необхідно враховувати недоліки нейронних мереж, а саме:

- неточність – нейронній мережі властиво помилятися, з тим чи іншим шансом;
- оптимальність – для імплементації модуля необхідне довготривале тестування в безпечних умовах;
- невідома кількість даних для достатньої точності виявлення образів.

Також варто відзначити і переваги нейронних мереж:

- адаптація – нейронна мережа здатна адаптуватись до зовнішніх умов, які постійно змінюються;
- здатність до самонавчання в реальному часі [4];

Висновки та перспективи.

Отже, особливостями використання аерофотозйомки в поєднанні з комп'ютерним баченням та нейронними мережами є безпека особового складу та простота освоєння, швидкість передачі інформації та її обробки, адаптивність модуля до умов навколишнього середовища та бойового завдання. Саме тому сучасні реалії порушують проблеми використання машинного навчання, особливо в умовах активних бойових дій. Використання дронів будь-яких класів дає колосальну перевагу, зберігає особовий склад та виправдовує витрати в тактичному та стратегічному планах військової розвідки. Швидка адаптація та винахідливість українців дає можливість швидко імплементувати нові технології, тестувати їх в польових умовах і здобувати перевагу на полі бою. Проте не слід забувати, що будь-яка технологія потребує ретельної розробки та часу на випробування перед тим, як потрапити до кінцевого користувача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. OpenCV documentation index. URL: https://docs.opencv.org/. (Дата звернення: 13.11.2022р.).
2. Війна дронів. Які безпілотники використовують ЗСУ. URL: https://suspilne.media/250485-viina-droniv-aki-bezpilotniki-vikoristovuut-zsu-i-cim-voni-krasi-za-rosiiski/. (Дата звернення: 13.11.2022р.).
3. ЗСУ показали на що дійсно здатний Bayraktar TB2 Express. URL: https://defence-ua.com/news/zsu_pokazali_na_scho_dijno_zdatnij_bayraktar_tb2_pobachiti_tsil_za_50_km_ta_navesti_artileriju-6505.html. (Дата звернення: 13.11.2022р.)
4. Кутковецький В. Я. Розпізнавання образів: навчальний посібник / В. Я. Кутковецький. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2017. – 420 с
5. Ядро TensorFlow. URL: https://www.tensorflow.org/overview. (Дата звернення: 12.11.2022р.).

Гордієнко К.О. (ДУТ)

ОСНОВНІ ПОСТКВАНТОВІ КРИПТОГРАФІЧНІ АЛГОРИТМИ ТА НЕОБХІДНІСТЬ ЇХ ЗАСТОСУВАННЯ

Актуальність:

Історія квантових обчислень почалась з 1980-х років. Наразі, хоча вже існують квантові комп'ютери базовані на фотонах, і навіть їх комерційні версії, широкого поширення вони не набули і наразі використовуються для експериментів та вузькоспеціалізованих задач. Заглядаючи у майбутнє, вже розроблений математичний апарат, який можна назвати «постквантові криптографічні алгоритми». Такі алгоритми створені для забезпечення безпеки даних в той період часу, коли квантові комп'ютери зможуть легко обходити нинішні безпекові стандарти. Проте, постквантові криптографічні алгоритми можна реалізувати і використовувати вже зараз.

Постановка задачі:

В даний момент часу постає проблема безпечної передачі інформації і підтвердження її достовірності. На протязі існування цивілізації, з моменту виникнення писемності та формування складних соціальних структур, для передачі певної інформації для закритого кола осіб використовувались найпростіші криптографічні алгоритми, засновані на зміщення алфавіту або підстановці символів (або групи символів) замість певних визначених символів.

Зараз, з розвитком цифрових технологій, криптографічні алгоритми поділяються на симетричні, коли зашифровуються самі дані, та асиметричні, коли використовую пара відкритого та закритого ключа що використовуються для кодування та декодування інформації.

При створенні і розповсюдженні квантового комп'ютера, через особливості його логіки обчислень, криптографічні алгоритми асиметричного шифрування перестануть забезпечувати секретність і достовірність переданої інформації, що є великою вразливістю в майбутньому.

Мета:

Метою є дослідження існуючих математичних апаратів та заснованих на них деяких постквантових криптографічних алгоритмах.

Основні положення:

В XXI столітті набули великого розвитку дослідження квантових комп'ютерів – обчислювальних пристроїв, що ґрунтуються на принципах квантової механіки, принципу суперпозиції та квантової заплутаності. Якщо простий комп'ютер оперує умовною одиницею «біт» , квантовий комп'ютер використовує квантові біти, або «кубіт». Кубіти, на відміну від бітів, можуть бути одночасно в багатьох станах, таким чином обчислюючи не точні значення, а ймовірності. Проте, повторюючи обчислення, збільшується імовірність отримати правильну відповідь.

Проблема того як саме працює квантовий комп'ютер, така ж складна як і пояснити як працює людський мозок. Проте, вже існують перші мови програмування для квантових комп'ютерів, а також створено квантові комп'ютери с процесорами в сотні кубітів.

Як тільки квантові комп'ютери досягнуть квантової переваги, тобто здатності за більш короткий час виконувати обчислення ніж комп'ютери зі звичною бітовою архітектурою (а отже, в тому числі і суперкомп'ютери), тоді стає можливим несанкціоноване дешифрування результатів роботи асиметричних криптографічних алгоритмів.

Ця проблема стоїть особливо гостро, так як наразі, найбільш поширеними є саме асиметричні криптографічні алгоритми, що забезпечують достовірність передачі інформації в мережі Інтернет. Так як такі алгоритми працюють з парами двох ключів – відкритим (публічним) та приватним, маючи лише публічну частину ключа можна обчислити приватну частину, і таким чином дешифрувати всю передану інформацію.

На даному етапі розвитку, процесорних потужностей не вистачає для розшифрування криптосистем з відкритими ключами, заснованими на факторизації великих чисел, дискретному логарифмуванні або дискретному логарифмуванні за еліптичною кривою. Злам таких криптосистем можливий лише через метод «грубої сили», тобто перебором всіх можливих вхідних значень, що для звичайного комп'ютера займає дуже багато часу. Проте, квантові комп'ютери дозволяють виконувати перелічені вище операції в декілька разів швидше, при наявності необхідної кількості кубітів і використанні алгоритму Шора.

Алгоритми з симетричними ключами, а також алгоритми гешування, потенційно вразливі перед квантовим комп'ютером що буде застосовувати метод «грубої сили» за алгоритмом Гровера. Наприклад, алгоритм AES128 для зламу потребує 2^{256} операцій, проте квантовий комп'ютер справиться з цим завданням за 2^{64} операції.

Теоретично, з цим можна боротись, збільшуючи (або подвоюючи) розмір ключів (обчислюваної геш-функції), а також використовуючи сертифікати з дуже коротким терміном валідності. Проте, зі збільшенням потужностей квантових комп'ютерів такі криптосистеми також будуть піддаватись зламу.

Наразі пропонуються два варіанти вирішення такої проблеми – використання квантових криптографічних алгоритмів, що враховують квантову фізику, а отже, теоретично захищені від атак квантовим комп'ютером.

Інший підхід – це використання постквантових криптографічних алгоритмів, що засновані на обчислювально-складних криптопримітивах для квантових комп'ютерів. Такі криптографічні алгоритми можна розгортати на звичайних комп'ютерах з бітовою архітектурою, а отже придатні до реалізації і застосування вже зараз, враховуючи особливості логіки роботи квантових комп'ютерів та алгоритми Шора і Гровера.

В наші дні, відсутня чітка стандартизація постквантових криптографічних алгоритмів. Цим питанням займається ETSI (Європейський інститут телекомунікаційних стандартів) та NISA (Національний інститут стандартів та технологій США). Серед існуючих пропозицій алгоритмів, які зараз досліджуються робочими групами вищевказаних інститутів, можна виділити наступні категорії криптопримітивів:

- Hash-based – криптографічні алгоритми, засновані на використанні геш-функцій та побудові дереві Меркла. Для безпеки використання використовують одноразові підписи за схемами Лемпорта-Діфі або Вінтерніца. Кожен вузол дерева – це конкатенація дочірніх вузлів дерева. Кореневий вузол – послідовно розрахований відкритий ключ. Листя – значення одноразових ключів. Таким чином, за допомогою одного відкритого ключа, можливо використовувати багато приватних ключів, не переживаючи за їх компрометацію. Серед недоліків – великий розмір ключів та довгий час генерації відкритого підпису. Відомі реалізації – SPHINCS, XMSS
- Code-based – криптосистеми з виправленням помилок. До корисних даних, що потребують їх передачі, в певний спосіб додається «надлишкова» інформація (наприклад, контрольне число). Під час зчитування даних, надлишкова інформація використовується для виявлення та виправленням помилок. Кількість помилок обмежена реалізацію алгоритму. Відомі алгоритмі шифрування даного типу – McEliece, QC-MDPC (один з варіантів McEliece)
- Multivariate – криптопримітив, що базується на розв'язанні систем багатовимірних поліномів. Передбачається безпечне застосування алгоритмів на основі цього криптопримітиву, допоки не буде доведено що розв'язання квантовому комп'ютерами задач такого типу є більш легким ніж для звичайного комп'ютера. Можна використовувати для цифрових підписів. Наразі, реалізації невідомі.
- Lattice-based – алгоритми асиметричного шифрування, за основу яких лежать завдання з теорії алгебраїчних решіток (дискретних підмножин векторів у евклідовому просторі R^n, що замкнені відносно операцій додавання та віднімання векторів). Такі

алгоритми є відносно простими і легкими для розпаралелювання обчислень для шифрування/розшифрування повідомлень, а також генерації і верифікації цифрових підписів. Недоліком таких алгоритмів є складність оцінки безпеки. Відомі реалізації – NTRUEncrypt, Falcon, Kyber, SWIFFT,

- Isogenies – криптопримітив, заснований на задачі оцінювання ізогенії суперсингулярних еліптичних кривих. Хоча задачі дискретного логарифмування на еліптичних кривих можливо ефективно розв'язати на квантових комп'ютерах з використанням алгоритму Шора, проте відсутня квантова атака для задач оцінки ізогенії на суперсингулярних кривих. Такий алгоритм можна використовувати та шифрування/дешифрування, створення пар відкритого та приватного і цифрових підписів. Наразі, реалізації алгоритмів на базі такого криптопримітиву невідомі.

Висновок

Можливе створення потужного квантового комп'ютера ставить під загрозу безпеку використання широкорозповсюджених криптографічних алгоритмів, що наразі використовуються для реалізації цифрових підписів, формування ключів, шифрування інформації, і відграють вирішальну роль в безпечній, конфіденційній і неспотвореній комунікації в мережі Інтернет, і в будь-яких галузях де потрібна безпека інформації.

Інформація що передається зараз або в майбутньому є вразливою для підслуховування, і може зберігатись до часів розвитку і розповсюдження квантових комп'ютерів що дозволять провести розшифровку даних за прийнятну кількість часу.

Для забезпечення від несанкціонованого доступу до даних, необхідно вже зараз працювати над впровадження заходів безпеки з використанням наявних криптопримітивів, що відносяться до постквантових криптографічних алгоритмів. Таким чином, за наявної матеріальної бази, можливо покращити поточний безпековий рівень, а також убезпечити себе від можливих майбутніх атак з використанням квантового комп'ютера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alagic, G. , Cooper, D. , Dang, Q. , Dang, T. , Kelsey, J. , Lichtinger, J. , Liu, Y. , Miller, C. , Moody, D. , Peralta, R. , Perlner, R. , Robinson, A. , Smith-Tone, D. and Apon, D. (2022), Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8413, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458 (Accessed November 14, 2022)

2. ETSI White Paper No. 8 Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges June 2015 ISBN No. 979-10-92620-03-0 Bernstein, D.J. (2009). Introduction to post-quantum cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_1

3. Shor, P. W. (1994, November). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124–134). IEEE.

4. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42–44, pp. 114– 116.

5. Alagic, G. et al. (2019). Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf.

6. Кравченко П. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 3 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2022

7. Горбенко, Ю. І.; Ганзя, Р. С. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. Вісник Національного університету Львівська політехніка. Комп'ютерні системи та мережі, 2014. Режим доступу: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_9

Гримуд А.Г. (ВІТІ ім. Героїв Крут)
д.т.н. Романюк В.А. (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ ПО ВИЗНАЧЕННЮ ТРАЄКТОРІЇ ПОЛЬОТУ ТА ТОЧОК (ІНТЕРВАЛІВ) ЗБОРУ ДАНИХ ТЕЛЕКОМУНІКАЦІЙНОЮ АЕРОПЛАТФОРМОЮ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

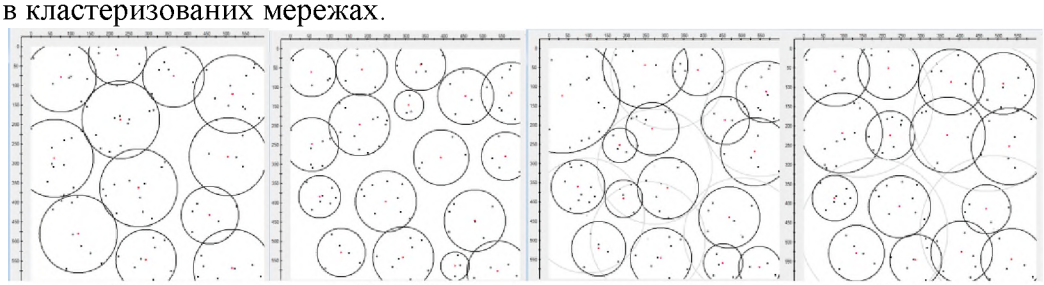
Збір даних у безпроводових сенсорних мережах (БСМ) викликав багато публікацій науковців завдяки прискореному розвитку Інтернету речей. Телекомунікаційна аероплатформа (ТА) на базі безпілотного літального апарату володіє високою рухливістю і гнучкістю та розглядається як перспективна технологія для збору даних у БСМ, особливо в умовах відсутності зв'язності між вузлами мереж або її шлюзом. Фактично ТА виступає в ролі мобільного шлюзу та має можливість збирати дані з кількох вузлів за зонами покриття. Динамічне формування кластерів та їх розмірів, траєкторія переміщення ТА, локація точок та інтервалів обміну ТА даними з вузлами суттєво впливає на ефективність збору даних. Більшість існуючих досліджень або нехтують цією проблемою або поділяють мережу на зони обслуговування ТА заданого розміру, що призводить до збільшення часу збору даних або збільшення витрат енергії батарей вузлів. Тому пропонується ієрархічна модель прийняття рішень по визначенню траєкторії польоту та визначенню точок (інтервалів) збору даних ТА за рівнями: мережа, кластер, ТА-вузол (рис. 1).

Рис. 1 – Процес прийняття рішень по траєкторії і точкам (інтервалам обміну)

На рівні мережі на відміну від існуючих підходів, де проводиться тільки однорідна кластеризація (наприклад, використовується алгоритм кластерного аналізу FOREL), додатково запропоновано проводити неоднорідну кластеризацію. При цьому враховуються параметри стану вузлів кожного кластеру, взаємне розташування кластерів (рис. 2) для прийняття рішення по виключенню кластера або його додатковому розбиттю. Це дає можливість в залежності від цільових функцій (ЦФ) знизити витрати енергії батарей за рахунок зменшення розміру кластера або зменшення часу збору даних (за рахунок його збільшення).

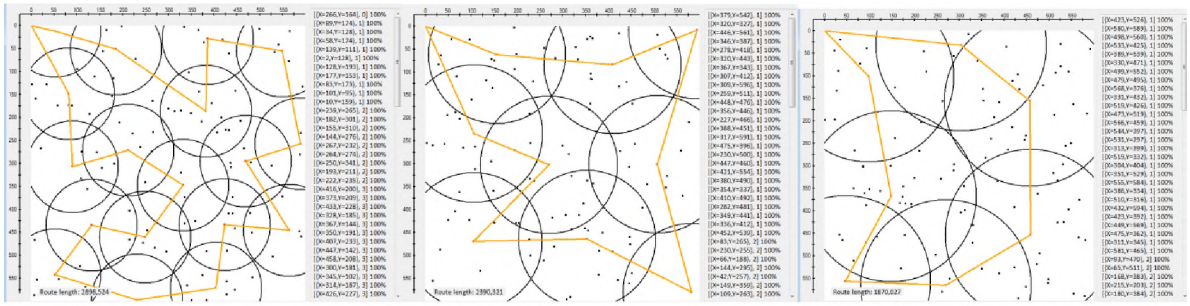
В якості первинної стратегії обльоту визначається обліт та збір даних ТА через центри кластерів. Будується маршрут обльоту (рішення задачі комівояжера) точок збору даних в

мережі за алгоритмом Convex Hull Insertion Heuristic (CHIH) (рис. 3), який показав кращі результати в кластеризованих мережах.



R=80 *R*=100 *R*=150 *R*=190

Рис. 2 – Варіанти кластеризації БСМ з різними радіусами *R* покриття ТА

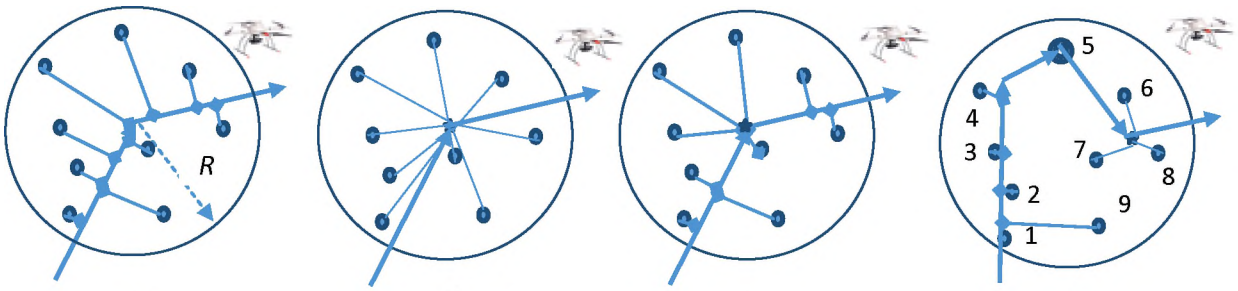


R=100 *R*=150 *R*=190

Рис. 3 – Результати реалізації алгоритму пошуку маршруту CHIH

На рівні кластеру визначено алгоритм знаходження декілька точок збору даних ТА у просторі кожного кластеру, який на відміну від існуючих враховує фактичний обсяг даних, наявну енергію батарей вузлів в кластері та параметри MAC-протоколу. Це дозволяє мінімізувати середні витрати енергії вузлів кластеру або мінімізувати час обміну даними. Це стає можливим завдяки знаходження оптимального положення ТА у просторі над вузлами кластеру згідно пріоритету цільової функції. Незначна обчислювальна складність запропонованого алгоритму $O(n_{\text{point}}n^2)$ дозволяє ТА використовувати його в реальному часі.

На рівні ТА-вузол кластера – визначається стратегія його обльоту та збору даних ТА (рис. 4: а –в процесі польоту; б – зависання в центрі кластеру; в – гібридна, в польоті з зависанням; г – гібридна, декілька точок зависання в врахуванням ЦФ) з врахуванням стану вузлів. Для вибору оптимальної стратегій обльоту вузлів розроблена відповідна база правил.



а *б* *в* *г*

Рис. 4 – Основні варіанти стратегій польоту та збору даних ТА з вузлів в кластері

Таким чином, досягнення результату відбувається за рахунок поетапної багатокритеріальної оптимізації за рівнями ієрархії (мережа, кластер, вузол) з врахуванням цільових функцій управління процесом збору даних. Результати імітаційного моделювання показав можливість зменшити час збору даних на 10–15% або підвищити часу функціонування мережі на 12–17% при задоволенні ресурсних обмежень. Важливо відмітити, що запропонована модель може бути використаний в спеціальному програмному забезпеченні системи управління ТА, центру управління мережею. Також її обчислювальна складність дозволяє застосовувати ТА в масштабі реального часу.

Громлюк К.А. (ВІТІ ім. Героїв Крут)
Зінченко І.А.(ВІТІ ім. Героїв Крут)
Фещенко І.О. (НДІ ВР)

ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ СИНТЕЗУ МЕТОДУ ФОРМАЛІЗАЦІЇ АНАЛІТИЧНОГО ОПИСУ СИСТЕМИ ВІЙСЬКОВОГО ЗВ'ЯЗКУ

Вторгнення в Україну 2022 року показало важливість створення інформаційної переваги, що надає можливість територіально розосередженим силам лишатися добре інформованими про загальну обстановку, як власних, так і суміжних підрозділів. У таких умовах ведення бойових дій активно застосовується концепція мережецентричних операцій, де важливого значення набуває завдання своєчасного планування і розгортання інформаційно-комунікаційної мережі поля бою (системи військового зв'язку), що згідно з керіними документами країн-парнерів є мережами класу C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance& Reconnaissance). Відтак, важливого значення набуває забезпечення ефективного виконання завдань органом управління зв'язком.

Система військового зв'язку складається із поєднання різних мереж родів та видів зв'язку. Мережі родів зв'язку поєднують між собою вузли зв'язку і де-факто, разом з вузлами зв'язку, утворюють інфокомунікаційну транспортну мережу (первинну систему зв'язку). До мереж родів зв'язку відносяться мережі супутникового, тропосферного, радіорелейного, радіо, проводового зв'язку. Мережі родів зв'язку накладаються одна на одну, взаємно поєднуючи і резервуючи одна одну. Таким чином, вузли зв'язку різного призначення разом з мережами родів зв'язку утворюють топологію системи військового зв'язку. Таку топологію можливо аналітично описати і в подальшому використати одержані аналітичні вирази для потреби автоматизації процесів управління системою військового зв'язку.

Одним із часткових показників ефективності управління зв'язком є якість управління. Під якістю розуміється спроможність органу управління зв'язком забезпечити ефективну реалізацію бойових спроможностей військ зв'язку для успішного виконання ними завдань і досягнення мети забезпечення зв'язку в операції (бойових діях) з найменшими витратами та у визначені терміни.

Для опису часткових показників якості роботи органу управління зв'язком використовують імовірність інформаційної готовності органу управління зв'язком. Вона має лінійну залежність від кількості реалізованих для потреб управління системою зв'язку математичних моделей, інформаційних і розрахункових задач від їх потрібної загальної кількості.

Поточний досвід планування зв'язку у сучасних умовах спирається на застарілу графічну модель системи зв'язку, що передбачає нанесення графічних позначок елементів системи зв'язку на паперову карту. На даний момент такий підхід не дозволяє провадити автоматизацію процесів управління системою військового зв'язку. Тому питання розробки методу формалізації аналітичного опису системи військового зв'язку, який дозволить одержати математичні моделі для потреб управління військовим зв'язком, є дуже актуальним.

Наявність сучасних аналітичних моделей опису системи військового зв'язку буде слугуватиосновою для розробки інформаційних і розрахункових задач, які автоматизують процес прийняття рішення органом управління зв'язком. Наведене дозволить значно підвищити якість роботи органу управління військовим зв'язком.

Отже,завдання синтезу методу формалізації аналітичного опису системи військового зв'язку є актуальним науково-прикладним завданням дослідження і потребує вирішення. При цьому, у якості інструментарію дослідження, доцільно використати теорії графів і складних систем, загальну тензорно-матричну теорію і спеціальний математичний апарат торцевого добутку матриць.

Гурський Т.Г (А1906)
Березанський Д.О. (А1906)
Дубіль О.В. (ВІТІ ім. Героїв Крут)

ВЗАЄМОДІЯ РАДІОЗАСОБІВ РІЗНИХ ДІАПАЗОНІВ ЗА ДОПОМОГОЮ АПАРАТУРИ ВНУТРІШНЬОГО ЗВ'ЯЗКУ ТА КОМУТАЦІЇ RF-7800I ВИРОБНИЦТВА КОРПОРАЦІЇ L3 HARRIS З СИСТЕМОЮ СУПУТНИКОВОГО ЗВ'ЯЗКУ SLINGSHOT

Актуальність. На сьогоднішній день, для ефективного управління при веденні бойових дій, необхідно використовувати сучасні військові радіозасоби та обладнання, яке спроможне забезпечити голосовий зв'язок і передачу даних на велику відстань між мережами. Одним з таких засобів є система супутникового зв'язку SlingShot.

Метою є дослідження варіантів реалізації передачі голосу та даних між ультракороткохвильовими (УКХ) та короткохвильовими (КХ) засобами радіозв'язку.

Вклад основного матеріалу. SpectraSlingShot — це революційна система, яка унікальним чином перетворює УКХ-радіостанції на супутникову частоту L-діапазону, миттєво розширюючи їх радіус дії до BLOS (за межами прямої видимості).

Розроблений відповідно до вимог сил спеціальних операцій, SlingShot пропонує низку переваг для тих, хто бере участь у швидких операціях і потребує надійного та безперебійного зв'язку у русі.

SlingShot вже розгорнуто кількома країнами НАТО. Він має ранцеві, транспортні, морські та авіаційні системи. Це означає, що командування та контроль над усім персоналом, стає значно легшим.

Сутність пропозиції полягає в розробці технічного рішення, яке дозволяє організувати взаємодію між різнотипними радіозасобами різних країн виробників на великі відстані за допомогою додаткового обладнання.

Реалізація запропонованого технічного рішення досягається тим, що при відповідних програмних налаштуваннях та наявності кабелів з відповідними роз'ємами для підключення радіозасобів до системи супутникового зв'язку SlingShot, є можливість забезпечити наступні функціональні можливості:

- забезпечити зв'язок на великі відстані між підрозділами;
- забезпечити внутрішній зв'язок між членами екіпажу бойової машини;
- організувати зв'язок між членами екіпажу та зовнішніми абонентами з використанням радіостанції підключених до АВЗК;
- забезпечити можливість управління будь-якою радіостанцією, підключеною до АВЗК з робочих місць операторів;
- шлюзування між різнорідними радіомережами, що дає можливість об'єднувати цифрові КХ, УКХ радіомережі різних виробників між собою (за умови, що шлюзові радіостанції підключені до цієї системи).

Висновок. В даний час на озброєнні Збройних сил України перебуває велика кількість радіозасобів різних країн виробників, тому основною проблемою є їх сумісна робота. Виходячи з наявних засобів, що є на озброєнні, дану проблему можливо вирішити використанням системи запропонованої в даній роботі. Основною перевагою використання даного засобу є досить проста та інтуїтивно зрозуміла система налаштування апаратури під радіостанції, що будуть підключатися.

Дикий О.В. (ВІТІ ім. Героїв Крут)
Радченко М.М. (ВІТІ ім. Героїв Крут)
к.т.н. Данилюк І.А. (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ КОМПЛЕКС АВТОМАТИЗАЦІЇ ФУНКЦІЙ СЛУЖБОВИХ ОСІБ ВІДПОВІДАЛЬНИХ ЗА ОБЛІК ОСОБОВОГО СКЛАДУ В ОРГАНАХ УПРАВЛІННЯ ЧАСТИН ТА ПІДРОЗДІЛІВ МІНІСТЕРСТВА ОБОРОНИ ТА ЗБРОЙНИХ СИЛ УКРАЇНИ

На сьогодні завдання щодо удосконалення оборонного планування та управління життєвим циклом підрозділів, з'єднань, об'єднань та інших різноманітних структурних елементів Міністерства оборони України та Збройних сил України потребують втілення різноманітних способів автоматизації та штучного інтелекту, що дозволить оптимізувати, підвищити ефективність керування даними процесами та раціонально використовувати людський ресурс.

Запропонований програмний комплекс відноситься до інформаційних технологій, а саме до систем обробки, зберігання та відображення інформації, та може бути використаний в галузі автоматизації процесу ведення обліку особового складу та створення звітних документів в стройових та кадрових службах військових частин Збройних Сил України (далі – в/ч ЗС України).

Відомі системи ведення обліку особового складу та автоматизації роботи службових осіб в органах військового управління, з'єднаннях, військових частинах, вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів, установах і організаціях, на кораблях і в підрозділах ЗС України працюють згідно керівних документів наведених в джерелах [1; 2]. Вони [3; 4] реалізовані у вигляді спеціального програмного забезпечення Системи «Персонал», яка здатна забезпечити можливість створення, функціонування та розвинення захищеної ІТ-інфраструктури високого рівня щодо обліку особового складу. Але, нажаль, система «Персонал» не забезпечує автоматизацію ведення операційних процесів пов'язаних з обліком особового складу в підрозділах та створення звітної документації, з урахуванням необхідних критеріїв.

Пропонується автоматизувати операційні процеси кадрових та стройових служб, що підвищить якість та оперативність обліку особового складу та створення звітної документації з урахуванням індивідуальних особливостей кожної із в/ч ЗС України. Для цього був створений програмний комплекс "СКАТ" (надалі, програмний комплекс) (Фіг.1), який складається з програмних модулів, пов'язаних між собою, та дозволяє здійснити автоматизацію процесів під час здійснення обліку особового складу, оптимізувати та підвищити ефективність роботи стройових та кадрових служб в/ч ЗС України.

Запропонований програмний комплекс реалізований у вигляді двох функціональних складових (Фіг.2): серверної (програма з базою даних) та клієнтської (робочі місця).

Серверна складова (Фіг.3) (програма та база даних) забезпечує виконання наступних функцій:

створення єдиного захищеного середовища зберігання даних;

виконання програмного коду програми;

постійний доступ користувачів до програми;

нормалізація даних (за обсягом та структурою);

можливість модернізації системи через зміну функціональних потреб користувача чи модернізацію обладнання.

контроль за змінами даних на сервері;

аутентифікація користувачів та захист інформації від несанкціонованого доступу;

використання захищеного протоколу функціонування програми (https).

Клієнтське робоче місце (Фіг.4) забезпечує виконання наступних функцій:

ведення штатного та списочного складу військової частини;

ведення облікової картки військовослужбовця військової частини;

ведення електронних журналів обліку, а саме:

- формування відомості бойового та чисельного складу;
- формування вислуги років військовослужбовця на обрану дату;
- формування відомостей обліку військовослужбовців;
- формування звітних форм;

реєстрація користувачів та розподілу дозволів (ролей) користувачам;

незалежність від операційної системи, яка використовується користувачем.

Вихідним результатом роботи програмного комплексу є автоматизована структуризація обліку особового складу в/ч ЗС України з визначенням таких особливостей як:

- військові звання та їх типи;
- звітність, щодо кількісного та якісного стану особового складу.

Кінцева схема програмного комплексу автоматизації функцій службових осіб, відповідальних за облік особового складу в органах управління частин та підрозділів Збройних Сил України, щодо взаємодії його об'єктів приведена на Фіг. 5.

User – користувач (службова особа) який відповідальний за облік особового складу в органах управління частин та підрозділів Збройних Сил України.

Browser – веб-браузер (Google Chrome) який використовується на персональних комп'ютерах робочих місць користувачів.

Authentification - авторизація та автентифікація – підтвердження того, ким є користувач на вході, проходження перевірки автентичності та надання дозволу користувачу на вчинення дій, які визначені в системі.

Web server - веб-сервер – програма яка забезпечує зв'язок між клієнтом і базою даних з використанням певного протоколу для кодування запитів і відповідей клієнту.

Router - роутер - програма для обробки запитів з веб-сервера до контролера.

View - програмний модуль представлення даних для веб-сервера від моделі та роутера.

Controller - контролер – програмний модуль який відповідає за збір та обробку даних від моделі та роутера.

DB - база даних – місце для збереження даних в нормалізованому та оптимізованому вигляді.

Model - модель – програмний модуль, який відповідає за те в якому вигляді надавати дані від їх бази.

Користувач з робочого місця звертається до браузера, проходить авторизацію та автентифікацію, після чого отримує доступ для роботи з веб-сервером. Робота з веб-сервером полягає у наданні користувачу, у відповідь на його запити, представлення даних у формах, які вимагає користувач.

Таким чином, використання запропонованого програмного комплексу дозволить уникнути ручної та паперової роботи за рахунок автоматизації операційних процесів кадрової та стройової служб, що підвищить якість та оперативність обліку особового складу з урахуванням особливостей в/ч ЗС України, а також, за рахунок усунення суб'єктивного фактору, дозволить автоматизувати та підвищити ефективність, продуктивність та безпеку виконання функцій збереження, валідації, передачі даних та виконання документообігу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ МО України від 26.05.2014 № 333 «Про затвердження Інструкції з організації обліку особового складу Збройних Сил України». https://zakon.rada.gov.ua/laws/show/z0611-14#Text (дата звернення: 30.07.2022 р.)

2. Наказ МО України від 14.09.2018 № 464 «Про затвердження Змін до Інструкції з організації обліку особового складу Збройних Сил України». https://zakon.rada.gov.ua/laws/show/z1137-18#Text (дата звернення: 30.07.2022 р.)

3. Сініцин І. / Кейс Міноборони: управління персоналом в електронному вигляді // Електроний ресурс видання «Юридична Газета online» від 16 лютого 2018 року / Ігор Сініцин. https://yur-gazeta.com/publications/practice/inshe/keys-minoboroni-upravlinnya-personalom-v-elektronnomu-viglyadi.html (дата звернення: 30.07.2022 р.)

4. Електронний ресурс ТОВ "Софтлайн ІТ". https://softline.org.ua/ (дата звернення: 30.07.2022 р.).

д.п.н. Діденко О.В. (НАДПСУ)
д.п.н. Козубцов І.М. (ВІТІ ім. Героїв Крут)

ОСУЧАСНЕНА МОДЕЛЬ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ОФІЦЕРІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ НА ЗАСАДАХ ПОТРЕБ БОЙОВОЇ ПРАКТИКИ

Постановка проблеми. Майбутня діяльність офіцерів сектору безпеки та оборони України характеризується наявністю постійної небезпеки, пов'язаної з ризиком для життя, вимагає від офіцерів мужності, витримки, здатності подолати страх, готовність до самопожертви. У зв'язку з цим, офіцер перш за все повинен володіти високим рівнем свідомості, патріотизму, готовністю виконати свій обов'язок перед Батьківщиною, хоч б чого це коштувало. Недоліки існуючої моделі підготовки проявилися з перших днів повномасштабної військової агресії Російської Федерації (РФ) проти України в неготовності молодих випускників. Враховуючи зазначене, **метою доповіді** є на основі виявлених проблем та сучасних потреб бойової практики запропонувати осучаснення моделі підготовки офіцерів для потреб сектору безпеки та оборони з високим рівнем готовості до майбутньої професійної діяльності (служби) пов'язаної з ризиком для життя.

Результат дослідження. Для досягнення мети у вирішенні науково-практичного завдання необхідно з'ясувати:

по-перше, яким чином при «вступній компанії» до ВВНЗ серед багатьох кандидатів розпізнати потенційного майбутнього офіцера;

по-друге, яким чином вибудувати освітній процес у такій логічній послідовності, щоб підготувати високопрофесійного офіцера, готового до майбутньої професійної діяльності (служби) пов'язаної з ризиком для життя та сформувати особистість у відповідності до потреб бойової практики визначених Замовником.

Останнім трендом є впровадження в систему підготовки офіцерського складу нове поняття «професійна військова освіта» на засадах «лідерства», то очевидно, що на кожному етапі навчання має бути оцінювання індивідуальних лідерських якостей та рівня професійної та військово-спеціальної компетентності за якими має буде відсіювання потенційних кандидати. Цього не достатньо.

У запропонованій осучасненій моделі підготовки офіцерів для потреб сектору безпеки та оборони, ставка в досяганні успіху робиться на мотиваційний компонент. Через мотиваційний компонент учасники освітнього процесу зможуть сприяти у забезпеченні відсіювання потенційних майбутніх кандидатів у офіцерів з високими морально-діловими якостями та готовності до майбутньої військово-професійної діяльності у секторі безпеки та оборони в умовах бойових дій та високого ризику для життя.

Одним з етапів підготовки має бути обов'язкове складання самоаналізу кандидатом, де буде зазначено чи є в нього лідерські здібності до управління (менеджменту). Самооцінка власної мужності, патріотичного налаштування, самовладання в складних (нестандартних) ситуаціях, хоробрості, сміливість, рішучість, ініціативність та готовий брати на себе відповідальність за прийнятті командирські рішення та/або вчинені поступки. Свідоме розуміння кандидатом майбутньої ролі командира, як захисника вітчизни.

Висновки з даного дослідження.

Таким чином, можна сформулювати наступні висновки:

1. Відсутність рішень окремих суперечностей зі складу загальної проблеми і демонструє, що існуюча система вищої військової освіти підготувала офіцерів з низьким рівнем морально-ділових якостей та не зовсім готових відразу до майбутньої військово-професійної діяльності в умовах бойових дій протистояння повномасштабній військовій агресії РФ проти України.

2. Виконання бойових завдань, а також, організація повсякденної діяльності потребує адекватної системи кадрового менеджменту Збройних Силах України. Менеджмент в Збройних Силах України побудований на командно-розпорядчому підході. Офіцер – в першу чергу має стати провідним лідером топ-менеджером відповідного рівня управління.

Драглюк О.В. (ВІТІ ім. Героїв Крут)
Шаповал В.М. (ВІТІ ім. Героїв Крут)
Зарукін Г.Г. (ВІТІ ім. Героїв Крут)
Ковальчук Б.П. (ВІТІ ім. Героїв Крут)

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ УПРАВЛІННЯ БОЙОВИМИ ЗАСОБАМИ ШЛЯХОМ ВИКОРИСТАННЯ ДИНАМІЧНИХ ПРІОРИТЕТІВ ЗАЯВОК НА ОБСЛУГОВУВАННЯ

Із розвитком автоматизованих систем управління та впровадженням їх у всі сфери життєдіяльності істотно зростає роль операторів, що приймають рішення в цих системах. Ще важливіша ця роль у системах спеціального призначення, таких як автоматизовані системи управління бойовими засобами (АСУ БЗ), де час на прийняття рішення та доведення його до об'єкта управління є ключовим показником, від якого залежить як управління підрозділами (частинами) так життя військовослужбовців. Така задача на сьогоднішній день є актуальною і її рішення якої полягає в:

- автоматизації процесу підготовки необхідної і достатньої інформації для прийняття рішення;
- зменшенні часу введення-виведення інформації при взаємодії оператора і ЕОМ в процесі вироблення керуючого рішення;
- оптимізації інформаційної взаємодії оператора і ЕОМ за рахунок їх взаємної адаптації до конкретних задач та умов діяльності.

Важливою вимогою, що висуваються до АСУ БЗ, є стійкість управління, під якою розуміють здатність АСУ і її підсистем достатньо ефективно виконувати свої функції в умовах активного впливу противника на систему управління, в тому числі переміщення її елементів в ході бойових дій.

Зі стійкістю управління тісно пов'язана безперервність, тобто забезпечення операторів можливістю постійно впливати на хід бойових дій за рахунок своєчасного доведення до об'єктів управління (ОУ) розпорядчої інформації і отримання від них інформації про обстановку, що складається (заявок на обслуговування).

Основним критерієм оцінки безперервності управління є коефіцієнт безперервності керування який являє собою відсоткове відношення часу, на протязі якого виконується умова безперервності управління, до всього періоду, що розглядається.

Існуючі підходи спрямовані на забезпечення максимального коефіцієнту безперервності керування ОУ з максимальним пріоритетом, нехтуючи, для досягнення цього, безперервністю керування ОУ з меншими пріоритетами. Дані підходи виправдані, однак можуть спричинити втрату керування ОУ найнижчих пріоритетів через постійне ігнорування інформації про їх стан підсистемою управління. Окрім того, пріоритетне обслуговування заявок не враховує час доведення керуючих впливів до ОУ при нестабільному стані каналів зв'язку на інформаційних напрямках до ОУ нижчих пріоритетів через значне зростання часу доведення управляючих рішень (наказів, команд, розпоряджень) і неможливості його компенсації зменшенням часу прийняття рішення.

У результаті проведених досліджень, розроблена методика яка дозволяє усунути вказані недоліки шляхом створення динамічних пріоритетів вхідних заявок на обслуговування в процесі прийняття рішень, суть якого полягає у використанні прогнозованих значень пропускних спроможностей інформаційних напрямків телекомунікаційної мережі для формування динамічних пріоритетів заявок, що потрапляють на обслуговування людино-машинною системою.

Алгоритм який представлений в методиці, може бути використаний в АСУ БЗ різних видів та родів військ, при проектуванні автоматизованих робочих місць операторів управління бойовими засобами.

Думітраш В.О. (ВІТІ ім. Героїв Крут)
Думітраш О.В. (в/ч А0415)

РЕАЛІЗАЦІЯ ПРОТОКОЛУ OpenVPN В МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Сучасний розвиток інформаційних технологій в Збройних Сил України, зокрема мережі Internet, призводить до необхідності захисту інформації, що передається у рамках розподіленої мережі, що використовує мережі відкритого доступу.

При захисту інформацій в мережах спеціального призначення необхідно використовувати принцип глибоко ешелонної оборони від зовнішніх та внутрішніх загроз.

Відповідна стратегія передбачує необхідність створення багаторівневої системи захисту.

Створення системи захисту переданої інформації передбачає використання технології віртуальних приватних мереж (VPN).

Використання технології VPN в мережах спеціального призначення дозволяє забезпечити захищену передачу даних, технологія побудована на впроваджені спеціального програмного забезпечення та апаратних засобів.

Забезпечення інформаційної безпеки є актуальним насамперед для розосереджених військових підрозділів зі складною територіально-розподіленою та багаторівневою структурою.

Для вирішення зазначених цілей застосовуються такі методи захисту інформації, як реєстрація і протоколювання, ідентифікація і автентифікація, управління доступом, створення міжмережевих екранів та криптографія. Одним з останніх способів забезпечення міжмережевого захисту стали віртуальні приватні мережі - Virtual Private Network (VPN).

З їх допомогою створюються віртуальні канали зв'язку поверх мережі Internet. Вони дають можливість з'єднувати локальні мережі різних технологій та їх сегменти в одну мережу, а шифрування всього трафіку, що проходить по тунелю, здійснюється на канальному рівні моделі OSI. Шифрування забезпечує захист від доступу до інформації, що передається, а інкапсуляція не дозволяє зловмисникові з'ясувати адресата переданої інформації.

Проектування надійної мережі VPN неможливе без знання особливостей технології VPN. Тому необхідно розглянути загальні функції та принципи роботи VPN, провести класифікацію VPN за різними ознаками. Окрім цього, необхідно зробити обґрунтування вибору OpenVPN в якості продукта для організації мережі VPN для Збройних сил України.

Так, віртуальна приватна мережа (VPN, Virtual Private Network) – це логічна мережа, що створюється на базі загальнодоступних або віртуальних каналів інших мереж (наприклад, Internet). У VPN мережах застосовується технологія захисту інформації, заснована на міжмережевому екрануванні та захисті мережевого трафіка за допомогою криптографічних методів захисту інформації.

На рис. 1 зображено схему віртуальної захищеної мережі VPN.

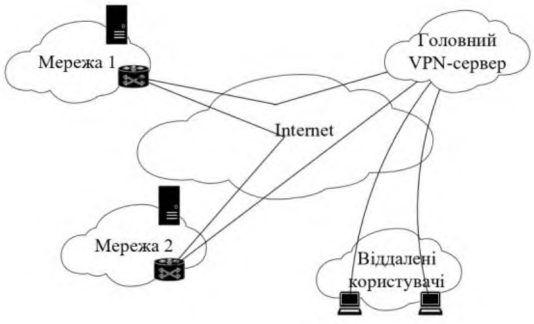


Рис. 1. Загальна схема VPN мережі

Основними цілями захисту інформації є унеможливлення або мінімізації ризиків реалізації загроз безпеки особистості, суспільства, держави внаслідок:

витоку, розкрадання, втрати, викривлення, модифікації, підробки інформації;

несанкціонованих дій по знищенню, викривленню, копіюванню, блокуванню інформації у комп'ютерних системах;

незаконного втручання в інформаційні ресурси й інформаційні системи;

порушення правового режиму документованої інформації як об'єкта власності;

порушення конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, наявних в інформаційних системах;

витоку державної таємниці документованої інформації відповідно до законодавства;

порушення прав суб'єктів інформаційних процесів при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їх забезпечення.

До технічних засобів захисту інформації належать:

резервне копіювання і віддалене зберігання масивів важливих даних на додаткових серверах;

дублювання та резервування всіх підсистем мережі, що мають значення для цілісності даних;

створення можливості перерозподілу ресурсів в мережі у випадках виходу з ладу елементів мережі;

можливість використання резервних джерел живлення;

встановлення програмного забезпечення, що забезпечує захист баз даних та конфіденційної інформації від несанкціонованого доступу.

Таким чином, введення в дію нових національних стандартів на OpenVPN дозволить суттєво удосконалити показники ефективності систем захисту, засобів і протоколів криптографічного захисту інформації, які розробляються в Україні, а в деяких випадках поліпшити їх порівняно з існуючими та перспективними світовими практиками. Особливо для роботи з інформацією з обмеженим доступом (ІзОД) є дуже важливим наявність такої системи, заснованої саме на національних стандартів криптографічного захисту інформації.

к. н. держ. упр. Живило Є.О. (ВІТІ ім. Героїв Крут)
Суднік В.О.(ВІТІ ім. Героїв Крут)

МЕТОДИКА ОЦІНЮВАННЯ СПРОМОЖНОСТЕЙ ВІЙСЬКОВИХ ЧАСТИН ТА ПІДРОЗДІЛІВ КІБЕРЗАХИСТУ СИЛ БЕЗПЕКИ ТА ОБОРОНИ ПО ВИКОНАННЮ ЗАВДАНЬ З ВІДБИТТЯ ВОЄННОЇ АГРЕСІЇ В КІБЕРПРОСТОРІ

Інновації керували військовою стратегією з моменту зародження людства. Винахід пороху, органної гармати та двигуна внутрішнього згоряння мали величезний вплив не лише на тенденції розвитку військової стратегії, а й на всю хронологію світової історії. Не стало винятком і XX сторіччя. Інтернет, що розвивається, продовжує розширювати можливості інформаційних технологій. Але, як і інші великі винаходи, його можливості часто використовуються за для досягнення негативних цілей та результатів.

Сьогодні в ході повномасштабного російського вторгнення в Україну наше суспільство і держава зіткнулось з новою загрозою, яка має величезний військовий і геополітичний потенціал. За короткий проміжок часу вразливості які мали/ють єдині системи електронних комунікацій, системи управління технологічними процесами перетворились на ефективний імовірний набір реальних і потенційних загроз національній безпеці України у кіберпросторі [1]. Зазначені загрози здатні порушити штатний режим функціонування комунікаційних систем спеціальних користувачів, у тому числі зрив та/або блокування роботи системи, та/або несанкціоновану управління її ресурсами.

При цьому ключову роль в підтриманні сталого функціонування таких систем у складі Сил безпеки та оборони України відіграють військові частини та підрозділи кіберзахисту Збройних Сил України. Так, порядок організації проведення оцінювання спроможностей у Збройних Силах України, як елемент планування на основі спроможностей здійснюється з урахуванням підходів, прийнятих у держав-членів НАТО. Зазначена сфера застосування охоплює питання методології процесу організації проведення оцінювання спроможностей, визначення учасників цього процесу, процедури і порядку його проведення, взаємозв'язку з іншими процесами, використання результатів цієї діяльності [2].

Водночас через відсутність Закону України "Про національну безпеку України" (відбувається редакція) [3], яким будуть внормовані питання оцінювання спроможностей, буде передчасним затвердження будь-якої нормативно-правової бази, яка б врегулювала цей напрямок діяльності. За цих умов, представниками Міністерства оборони та Збройних Сил України одноголосно наголошується на необхідності розробки відповідних методик щодо прогнозування, виявлення та надання оцінки загрозам національної безпеки держави в кіберпросторі та через кіберпростір [4]. Окремо слід підкреслити необхідність визначення порядку організації проведення оцінювання спроможностей, розробці методики оцінювання спроможностей військових частин та підрозділів кіберзахисту Збройних Сил України по виконанню завдань з відбиття воєнної агресії в кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) 2163-VIII від 17.08.2022. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text;

2. Наказ Міністерства оборони України 22.12.2020 № 484 (Зареєстровано в Міністерстві юстиції України 16 лютого 2021 р. за № 196/35818), "Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони" z0196-21 від 22.12.2020. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0196-21#Text;

3. Закон України "Про національну безпеку України" (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) 2469-VIII від 15.06.2022. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text;

4. Наказ Міністерства оборони України від 01 квітня 2019 року № 10/ДСК "Про затвердження Основних напрямів підготовки до відбиття воєнної агресії у кіберпросторі (підготовки та ведення кібероборони) у системі Міністерства оборони України.

д.т.н. Журавський Ю. В. (ЖВІ імені С.П. Корольова)
Ph.D Налапко О.Л. (ЦНДІ ОВТ ЗСУ)
Балан Д.Д. (ВІТІ ім. Героїв Крут)

МЕТОДИКА БАГАТОКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ОЗБРОЄННЯМ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Вступ

Локальні війни та збройні конфлікти останніх десятиріч характеризуються високою динамікою ведення операцій (бойових дій) та значним обсягом різноманітної інформації, яка використовується в процесі функціонування системи управління військами та озброєнням. Зазначене обумовлює необхідність пошуку нових підходів для підвищення оперативності прийняття рішень посадовими особами при заданій їх достовірності.

Процес підтримки прийняття рішення полягає в генерації можливих альтернатив рішень, їх оцінці та виборі кращої альтернативи з множини. При виборі альтернатив доводиться враховувати велику кількість суперечливих вимог і, отже, оцінювати варіанти рішень за багатьма критеріями.

Ухвалення рішення в більшості випадків полягає в генерації можливих альтернатив рішень, їх оцінці та виборі кращої альтернативи. Прийняти «правильне» рішення − означає вибрати таку альтернативу з числа можливих, яка з урахуванням усіх різноманітних чинників і суперечливих вимог в максимальному ступені сприятиме досягненню поставленої мети. Таким чином, особи, що приймають рішення, вимушені виходити зі своїх суб'єктивних уявлень про ефективність можливих альтернатив і важливості різних критеріїв. Під критерієм ефективності прийняття рішення особами, що їх приймають, будемо вважати оперативність прийняття рішення із заданим ступенем достовірності.

Для вирішення проблеми формування узагальнених показників ефективності, використовуваних в оцінці різних альтернатив рішення, пропонується використати нечітко-можливісний підхід для формалізації невизначеності при прийнятті рішень. А *метою зазначеного дослідження* слід вважати підвищення оперативності прийняття рішень щодо стану об'єкту управління із заданою достовірністю.

Виклад основного матеріалу дослідження.

Вплив різних показників на оцінку варіантів з множини альтернатив пропонується здійснювати шляхом побудови конструктивної λ-нечіткої міри Сугено на кінцевій множині часткових показників. Для вирішення проблеми формування узагальнених показників оцінки стану об'єкту аналізу, що використовуються в оцінці різних альтернатив рішення, пропонується використати нечітко-можливістий підхід для формалізації невизначеності щодо стану об'єкту аналізу та вирішення багатокритеріальної невизначеності.

Переваги теорії можливостей, заснованої на ідеї нечіткої множини, полягає в тому, що вона дозволяє якісно описати судження, що характеризують невизначеність та моделювати неточність в процесі прийняття рішення щодо стану об'єкту аналізу.

При цьому інформація про параметри та зовнішнє середовище носять неточний, невизначений характер, особливо на етапах формалізації вихідних даних, що використовуються при прийнятті рішення.

Методика багатокритеріального оцінювання системи управління військами та озброєнням в умовах невизначеності складається з наступної послідовності дій:

1. Введення вихідних даних та формалізація багатокритеріальної оцінки. У зв'язку з цим припустимо, що можливості параметрів реалізації задані у вигляді нечітких множин.

2. Побудова оціночної функції. Враховуючи вищезазначене вважаємо, що часткові показники оцінки стану об'єкту управління будуть представлені у вигляді нечіткої події.

3. Формулювання узагальненого показника оцінки стану об'єкту управління. На даному етапі відбувається формулювання узагальненого показника оцінки стану об'єкту управління (E), що представляє собою деяку операцію над нечіткими подіями.

Це об'єднує часткові показники оцінки стану об'єкту. Узагальнений показник також враховує їх вплив на оцінку варіантів рішення на різних етапах процесу прийняття рішення.

Поширеним методом ранжування критеріїв за важливістю є призначення кожному з них значення ваги з наступною операцією згортки. Даний підхід, приводить до втрат в ефективності його застосування. Вказані втрати пов'язані з тим, що коефіцієнти в згортці часткових показників ефективності не враховують нелінійний характер впливу показників один на одного і в цілому на узагальнений показник оцінки стану об'єкту аналізу.

4. Побудова нечіткої міри Сугено. Для того, щоб подолати вказані недоліки та врахувати нечітко-можливісне представлення часткових показників оцінки стану об'єкту, вважається доцільним, при побудові узагальненого показника оцінки стану об'єкту, використовувати нечітко-можливісне згортання, засноване на нечіткій мірі та нечіткому інтегралі.

Врахування впливу сукупності різноманітних показників на оцінку варіантів з множини планується здійснювати шляхом побудови конструктивної λ-нечіткої міри Сугено на кінцевій множині часткових показників.

5. Здійснення операції нечіткої згортки узагальненого показника оцінки. Узагальнений показник оцінки стану об'єкту пропонується отримувати у вигляді нечіткого згортання, що дозволяє гнучко враховувати нелінійний характер впливу часткових показників, для чого використовуємо поняття нечіткого інтегралу по λ-нечіткій мірі Сугено.

В якості оціночної функції будемо вважати значення часткових показників оцінки стану об'єкту аналізу, наведених до безрозмірного вигляду з носієм нечіткої множини в інтервалі [0, 1]. На основі запропонованого підходу представлена методика вирішення багатокритеріальної невизначеності та вибору альтернатив стану об'єкту аналізу.

Зазначений підхід запропоновано використовувати у процесі підтримки прийняття рішень особами, що їх приймають. Запропонована методика дозволить підвищити оперативність прийняття рішень при збережені заданого ступеню достовірності. Розроблена методика є універсальною та може бути адаптована для оцінки стану об'єкту аналізу довільної архітектури та складності.

Новизна розробленої методики в тому, що: враховуються тип невизначеності про стан об'єкту управління; формування узагальнених показників оцінки стану об'єкту управління є універсальною процедурою. Представлення узагальнених показників оцінки стану об'єкту аналізу дозволяє проводити адаптацію під конкретне завдання; наявна удосконалена процедура зменшення множини можливих варіантів рішення щодо стану об'єкту.

Обмеженнями зазначеного дослідження слід вважати: врахування часових обмежень на передачу конкретного типу повідомлення (формалізованого донесення); наявність первинної бази даних; обмеження щодо якості каналів передачі даних.

Висновки

У цьому дослідженні проведено розробку методики багатокритеріального оцінювання системи управління військами та озброєнням в умовах невизначеності. Результати дослідження стануть у нагоді при:

– розробці нових алгоритмів управління в системах підтримки прийняття рішень;

– обгрунтуванні рекомендацій щодо підвищення ефективності оперативного управління військами та озброєнням;

– аналізі об'єктів моніторингу в ході ведення бойових дій (операцій);

– створенні перспективних технологій підвищення ефективності оперативного управління військами та озброєнням;

– оцінці адекватності, достовірності, чутливості науково-методичного апарату оперативного управління в системах підтримки прийняття рішень;

– розробці нових та удосконаленні існуючих моделей управління.

к.т.н. Завада А.А. (ЖВІ ім. С.П. Корольова)
Наумчак Л.М. (ЖВІ ім. С.П. Корольова)
к.т.н. Романчук М.П. (ЖВІ ім. С.П. Корольова)

МЕТОД ЕЛЕМЕНТНОЇ СЕГМЕНТАЦІЇ ОБРАЗІВ ОБ'ЄКТІВ АЕРОРОЗВІДКИ НА ОСНОВІ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Аналіз досвіду протистояння широкомасштабному російському вторгненню в Україну показує високу ефективність застосування як розвідувальних, так і ударних комплексів на основі безпілотних авіаційних комплексів (БпАК). Що обумовлює нагальну потребу створення розвідувально-ударних комплексів на основі БпАК та модернізацію вже існуючих авіаційних комплексів у відповідності до визначених оперативно-тактичних вимог. Актуальність даного питання обумовлюється перспективами суттєвого підвищення бойового потенціалу окремих підрозділів Збройних Сил України.

Створення розвідувально-ударних комплексів на основі БпАК повинні забезпечити можливість нанесення ударів по виявленим цілям як на передньому краю противника, так і на значних відстанях із виконанням ключової умови щодо оперативності та точності видачі цілевказівок для засобів вогневого ураження противника.

Одним з основних факторів, що впливає на точність даних цілевказівок є точність позиціювання безпілотного літального апарату (БпЛА), яку особливо складно забезпечити на достатньому рівні в умовах активного застосування противником засобів радіоелектронної боротьби. В свою чергу, оперативність видачі цілевказівок залежить від оперативності обробки великих обсягів матеріалів повітряної розвідки, отриманих з БпЛА, що обумовлює нагальну потребу використання автоматизованих засобів обробки та аналізу вхідних образів для обробки великого обсягу оперативної інформації з метою виявлення об'єктів ураження. Основною задачею при цьому є процес ідентифікації відмінностей у стані об'єкта чи явища в районі повітряної розвідки.

Доступні засоби автоматизованої обробки та аналізу матеріалів повітряної розвідки на основі класичних методів розпізнавання образів не дозволяють забезпечити необхідний рівень якості та оперативності розпізнавання зображень. Пріоритетним напрямом розв'язання зазначеної проблеми є розробка та застосування моделей на основі штучних нелінійних нейронних мереж для автоматизованого виявлення та розпізнавання зразків озброєння та військової техніки (ОВТ) противника. Підкласом даних мереж є згорткові нейронні мережі, що забезпечують достатнє узагальнення інваріантних ознак ОВТ при меншій обчислювальній складності.

З метою розвитку методів елементної сегментації образів об'єктів аеророзвідки на основі технологій машинного навчання в роботі запропоновано використання згорткових нейронних мереж для вирішення завдань виявлення та класифікації об'єктів ураження, їх семантичної та елементної сегментації; визначені вимоги до створення та наповнення баз даних об'єктів розвідки; висунуті умови підбору гіперпараметрів.

Головна проблема при застосування нелінійних нейронних мереж для вирішення завдань автоматизованого виявлення ОВТ противника за результатами обробки матеріалів повітряної розвідки полягає в тому, що більшість великих наборів даних не є загальнодоступними, а тренування згорткових нейронних мереж на малих наборах даних робить їх схильними до перенавчання, що не забезпечує достатнє узагальнення інваріантних ознак. В роботі проаналізовані основні шляхи вирішення даної проблеми.

Таким чином, використання згорткових нейронних мереж, що використовують підхід елементної сегментації, при автоматичній обробці зображень дозволять здійснювати розпізнавання об'єктів аеророзвідки в масштабі часу близькому до реального із високою достовірністю, в умовах активного застосування противником засобів радіоелектронної боротьби, що забезпечить необхідну точність та оперативність видачі цілевказівок для засобів вогневого ураження засобів противника.

к.т.н. Закіров С.В. (НДІ ВР)
к.т.н. Ірха А.В. (НДІ ВР)

ТЕХНІЧНІ АСПЕКТИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БОРОТЬБИ В ХОДІ ШИРОКОМАШТАБНОГО ВТОРГНЕННЯ ЗБРОЙНИХ СИЛ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В УКРАЇНУ

Актуальність. В сучасних умовах ведення збройних конфліктів одним з вирішальних факторів досягнення перемоги є домінування в інформаційному просторі. Це особливо важливо для України, яка змушена вести бойові дії з країною із переважаючим військовим потенціалом. Інформаційна війна проти України носить стратегічний характер та ведеться без обмежень у методах, просторі та часі. З початком військових (бойових) дій сили і засоби інформаційної боротьби російської федерації (рф) вирішують завдання з використанням усього можливого арсеналу ведення наступальної інформаційної операції [1].

Постановка задачі. Кожна зі складових ведення інформаційної операції включає широкий спектр заходів. В доповіді розглядається така важлива складова ведення інформаційної боротьби як радіоелектронна боротьба (РЕБ). Саме вона займає особливе місце під час ведення інформаційної війни через те, що її інформаційно-технічну основу складають радіоелектронні системи та засоби.

Метою доповіді є аналіз сучасних аспектів РЕБ як складової інформаційної боротьби в ході широкомасштабного вторгнення збройних сил рф в Україну на основі дослідження трофейних зразків.

Основні положення. У ході масштабної реформи збройних сил (зс) рф, що стартувала в 2008 році, була сформована система РЕБ. У всіх військових округах зс рф сформовані окремі бригади РЕБ. Окремі роти РЕБ є в кожній із мотострілецьких танкових бригад (дивізій), а також у складі більшості бригад та дивізій Повітряно-десантних військ. У Військово-морському флоті сили РЕБ об'єднані в окремі центри РЕБ. У Повітряно-космічних силах батальйони РЕБ входять до складу армій військово-повітряних сил та протиповітряної оборони [2]. Поряд із структурними реформами військ РЕБ відбулося їх переозброєння на нову сучасну техніку. В результаті цього були створені, прийняті на озброєння та надійшли до підрозділів модернізовані та нові технічні засоби РЕБ авіаційного, наземного та морського базування різного функціонального призначення, більшість яких застосовуються в ході бойових дій на території України.

Висновки. В доповіді розглянуті результати досліджень особливостей побудови та застосування сучасних трофейних зразків техніки РЕБ, які використовує рф в ході широкомасштабного вторгнення в Україну. В результаті ведення бойових дій отримані зразки потрапляють для дослідження в різному технічному та якісному стані від повністю знищених до цілком справних. Відповідно ступінь та детальність вивчення їх можливостей досить відрізняється. Дослідження складу трофейних зразків техніки РЕБ свідчить про те, що базові підходи до їх створення в росії не змінилися, хоч і ведеться постійне доопрацювання конкретних вузлів за рахунок використання готових модулів та радіокомпонентів іноземного виробництва, що є наслідком відсутності російських аналогів. Спостерігається зміна конструктивних рішень в зразках різних років (партій) виготовлення, що імовірно свідчить про дію санкційного тиску на комплектування виробничих потужностей.

В доповіді розглянуті далеко не всі зразки техніки РЕБ, які використовує рф в нападі на Україну. Це пов'язано з тим, що ряд засобів РЕБ рф використовує зі своєї території поза межами зони вогневого ураження зенітно-ракетних засобів ЗС України, що не дозволяє отримати їх для проведення досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – Харків: Консум, 2004. – 508 с.
2. Електронний ресурс. https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14231%40morfDictionary&ysclid=la7y4f6cdl398487806

к.т.н Захарченко І.В. (ХНУПС)
Захарченко В.В. (ХНУПС)
Дзюба І.В. (ХНУПС)
Гончаренко І.В. (ХНУПС)

МЕТОД ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ РАДІОЧАСТОТНИМ РЕСУРСОМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЙНОЇ МЕРЕЖІ

Актуальність. На сучасному етапі інтелектуалізація мережевого та абонентського обладнання є одним активних напрямків розвитку бездротових мережевих технологій. В умовах дефіциту спектру впровадження нових сервісів, шляхом використання вільних ділянок радіочастотного діапазону, стає досить складним і не завжди можливим завданням. Можливим шляхом вирішення вказаного завдання є реалізація динамічного управління спектром (частотним ресурсом) за рахунок надання можливості використання діапазонів первинних користувачів − вторинним користувача, на той період часу, доки вказаний діапазон не використовується первинним користувачем.

Постановка задачі. Методи ефективного використання радіочастотного спектру технології когнітивного радіо для цивільного призначення розглядаються в багатьох роботах. Однак питання впровадження вказаної технології для військових телекомунікаційних систем з урахуванням порядку застосування радіочастот для військового повітряного радіозв'язку знаходяться в стадії активних досліджень.

Метою роботи є підвищення ефективності застосування радіочастотного спектру інформаційно-телекомунікаційної мережі військового призначення за рахунок інтелектуального управління її радіочастотним ресурсом.

Основні положення. Управління радіочастотним ресурсом бездротової телекомунікаційної системи здійснюється з метою організації ефективного використання радіочастотного спектру, шляхом визначення вільних на даний момент часу ділянок радіочастотного діапазону первинних користувачів та передачі в них інформації вторинними користувачами. Такий підхід реалізує технологію "когнітивного радіо". Для цього здійснюється моніторинг сигнально-завадової обстановки, а саме − аналіз радіочастотного спектру на наявність радіосигналів від: радіосистем противника; систем радіоелектронної боротьби противника; радіосистем своїх військ, що працюють з відомими видами сигналів. Для реалізації управління радіочастотним ресурсом застосовується математичний апарат нечіткої логіки.

Інформація про порядок застосування радіочастот для військового повітряного радіозв'язку зберігається в базах даних військових телекомунікаційних систем і формується згідно відповідних керівних документів. При призначенні частот враховуються частоти, які включені до документів аеронавігаційної інформації, частоти єдиних радіомереж та радіомереж взаємодії, а також частоти, які заборонені для використання відповідною директивою Генерального штабу Збройних Сил України про заборону використання частот, а також діючі на території повітряних командувань центри ДМВ-ЧМ радіомовлення у діапазоні від 108 Мгц до 144 МГц.

Частоти, дозволені для використання, представимо лінгвістичною змінною "ДДЧ" (діапазон дозволених частот), базова терм-множина якої визначається множиною можливих значень: $T_{ДДЧ}$ ={"МХ1", "МХ2", "ДМХ1", "ДМХ2"} (варіант) з функціями приналежності П-подібної (колоколоподібної) форми (рис. 1).

Рис. 1 Терми ЛЗ "Діапазон дозволених частот"

ЛЗ "ДДЧ" зберігається в захищеній базі даних з обмеженням доступу до цієї інформації відповідними особами. В процесі функціонування бездротової інформаційно-телекомунікаційної системи цифровий панорамний спектральний аналізатор в режимі реального часу сканує навколишнє радіосередовище та виявляє ділянки радіоспектру, в яких здійснюється робота інших радіосистем.

Для виявлення зайнятих смуг частот у спектральному діапазоні, сумісно з цифровим панорамним спектральним аналізатором пропонується застосовувати BDS-виявлювач, що дозволить виявляти наявність сигналів при співвідношеннях сигнал/шум менших за одиницю. Робота BDS-виявлювача базується на застосуванні BDS-статистики, яка використовує статистичні властивості кореляційної розмірності процесу в фазовому просторі (аналіз "образу" сигналу). У випадку, якщо значення BDS-статистики виходять за межі встановленого інтервалу $[-1,96; 1,96]$, приймається рішення про наявність первинного користувача. Якщо значення BDS-статистики приймають значення у межах даного інтервалу, приймається рішення про вільність даного піддіапазону і відповідно можливості його застосування вторинним користувачем.

Вільні ділянки частот, отримані за даними панорамного цифрового аналізатору спектру та BDS-виявлювача когнітивного радіотерміналу представляються у вигляді лінгвістичної змінної "ДВЧ" (діапазон вільних частот), яка ініціалізується під час початку сеансу обміну даними. Базова терм-множина "ДВЧ" визначається множиною можливих значень: ДВЧ ={"1", "2", "3", 4", 5", 6"} з П-подібними (колоколоподібними) функціями приналежності термів, представленими на рис. 2.

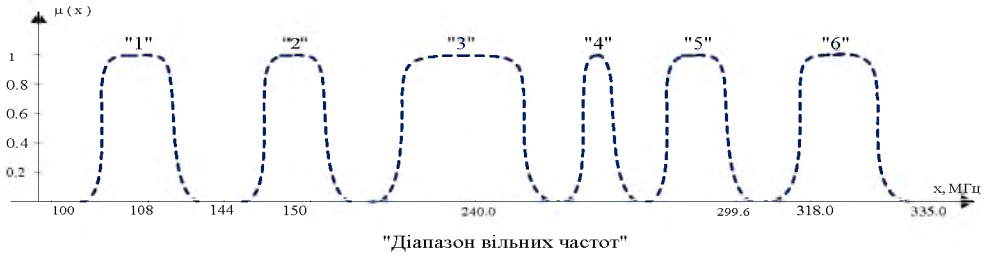


Рис. 2 Терми ЛЗ "ДВЧ"

Під час сеансу обміну даними кількісні значення ЛЗ "ДВЧ" адаптивно оновлюються у відповідності до стану навколишнього радіосередовища.

Визначення ділянок частот, в яких можлива передача інформації, а саме формування лінгвістичної змінної "ДРЧ" (діапазон робочих частот) здійснюється шляхом виконання операції перетину двох нечітких множин, перша з яких є діапазоном дозволених частот "ДДЧ", друга – діапазоном вільних частот "ДВЧ" (рис.3.та рис.4):

$$ДРЧ = ДДЧ \cap ДВЧ \qquad (1)$$

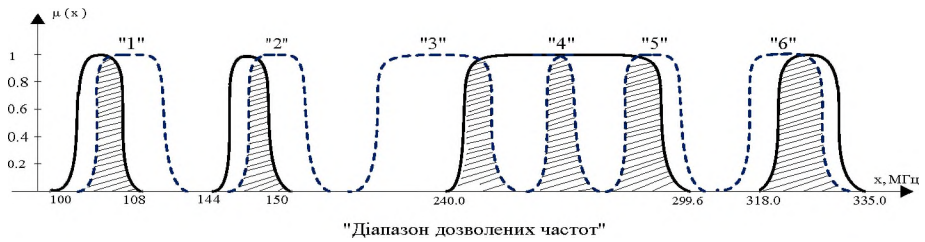


Рис. 3 Операція перетину ЛЗ "ДДЧ" та "ДВЧ"

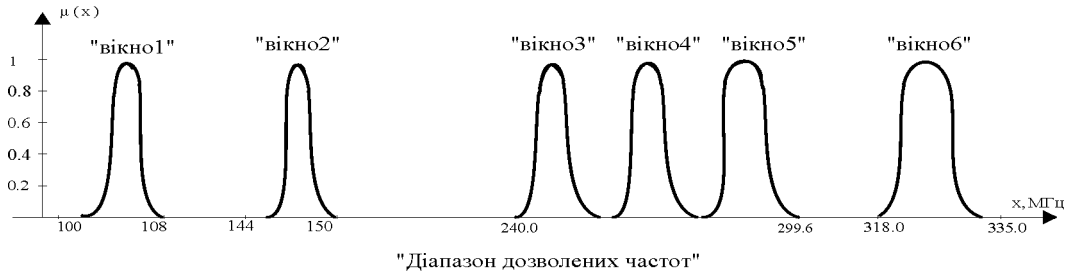


Рис. 4 Терми ЛЗ "ДРЧ"

Сформовані таким чином терми ЛЗ "ДРЧ" описують множину частотних вікон, кожне з яких характеризується своєю шириною W (МГц) в радіоспектрі. Вибір фактичного частотного вікна, в якому радіотермінал буде працювати в кожний момент часу буде здійснюватися відповідно до його пріоритету Pr, який призначається в залежності від його ширини W та рівня шумів L (мВт) в ньому. Найвищий пріоритет призначається вікнам з max W та min L. Найнижчий пріоритет − вікнам з min W та max L.

Вказані характеристики кожного частотного вікна (W, L, Pr) представляються у вигляді структури з відповідними полями, які зберігаються та оновлюються в базі даних. W та L визначаються цифровим спектральним аналізатором. Для призначення пріорітету Pr пропонується використовувати гібридну нейро-нечітку мережу у формі адаптивної системи нейро-нечіткого виводу ANFIS (adaptive neuro-fuzzy inference system), здатною до навчання. Для створення ANFIS мережі на етапі її проектування на основі експертних оцінок формується навчальна вибірка Pr(W,L), що відображає залежність значення пріоритету Pr від ширини вікна W (Мгц) та рівня шумів L (мВТ) в ньому. Модель сформованої адаптивної мережі представляє собою систему нечіткого виводу типу Сугено 0-го порядку (рис.5).

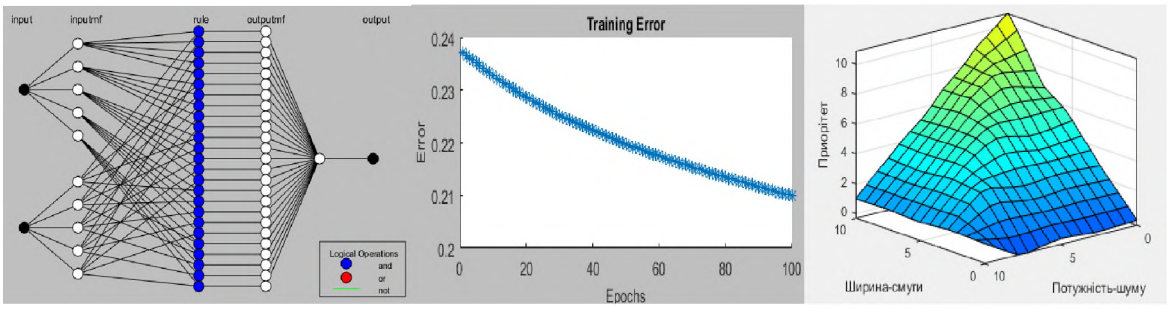


Рис.5 Структура ANFIS-моделі та результати її навчання

В процесі функціонування когнітивної бездротової системи цифровим аналізатором спектру виявляється множина вільних радіочастотних ділянок. Кожна з ділянок аналізуються BDS-виявлювачем на предмет наявності сигналів від радіозасобів, що працюють на рівні шумів. Якщо значення BDS- статистики свідчить про присутність таких радіосигналів, ці ділянки відкидаються. Якщо радіосигнал відсутній, ці ділянки приймають участь в формуванні термів ЛЗ "ДВЧ". Далі формується ЛЗ "ДРЧ". Після цього, навчена на етапі проектування, нейро-нечітка ANFIS-мережа здійснює призначення пріоритетів кожній з ділянок робочих частот для прийняття рішення, в якій з них здійснювати передачу радіосигналу.

Висновки. Розроблено метод управління радіочастотним ресурсом із застосуванням нелінійного аналізу часових спостережень (BDS – статистика) та гібридних нейро-нечітких мереж, для вибору ділянки радіочастотного спектру в межах якої можливо здійснювати передачу радіосигналів. Запропонований метод підвищує ефективність застосування радіочастотного спектру за рахунок надання сервісу за вимогами, тобто передачі інформації носіями на вільних у даний час частотах.

д.т.н. Зінченко О.В. (ДУТ)
Кисіль Т.М. (ДУТ)
к.т.н. Фесенко М.А. (ДУТ)

ІНТЕЛЕКТУАЛЬНИЙ ЗАСТОСУНОК МОНІТОРИНГУ ТА РОЗПІЗНАВАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ

На сьогоднішній день армії провідних країн світу в тому числі і України активно впроваджують у свою практику системи штучного інтелекту. Зокрема попитом користуються системи для проведення моніторингу та розвідки, аналізу потенційних загроз, а також збору інформації, необхідної для планування та проведення бойових операцій. Для виконання перелічених завдань можуть бути застосовані існуючі системи розпізнавання об'єктів (відеозображень), звуків тощо. Для цього існуючі алгоритми необхідно удосконалювати шляхом додавання нових даних та інформації щодо військової техніки й інших сучасних засобів військового призначення.

Фахівці кафедри штучного інтелекту Державного університету телекомунікацій, мають певні досягнення в цьому напрямку. Ними створений застосунок, здатний визначати потенційно загрозливі об'єкти противника під час оброблення відеоданих, звукових сигналів тощо. Застосунок спроможний в автоматичному режимі здійснювати захоплення динамічних об'єктів (техніки військового призначення), супроводжувати, ідентифікувати та видавати дані про їх наявність, а також отримання сповіщень про їх наближення до небезпечного об'єкту.

Мобільний застосунок, зорієнтований як для військовослужбовців, так і для громадського населення, працює на базі ML-технологій та розпізнає за фотографіями техніку військового призначення в режимі реального часу. Перевагою даної технології є інноваційні способи: переконфігурації та інтеграції обладнання, програмного забезпечення та їх взаємозв'язку; збору та аналізу великих обсягів даних, безперешкодної взаємодії між інтелектуальними машинами та віртуалізацією об'єктів, що дозволить здійснювати незалежну самокорекцію відповідно до інформації, отриманої на геолокаційних інтерактивних картах.

Згідно із поданою концепцією, карти повинні допомагати у виявленні просторових зразків, завдяки автономному пошуку та виявленню цілей у визначеному секторі влучень, оцінки ступеня їх загрози, супроводу та визначення параметрів її руху, розробки цифрової системи, що зможе візуалізувати, а відтак і управляти геопросторовими даними у зручному для середовищі.

До таких дій слід віднести дистанційну роботу, яка включає декілька етапів функціонування:

- *Збір даних.* На першому етапі необхідно провести збір всіх даних, після чого їх поєднують із загальнодоступними даними об'єктів військового призначення та поточною інформацією, яка буде передаватись в режимі реального часу. Згідно зібраних даних та регулярного їх оновлення будуть прогнозуватись траєкторії польоту та місця вражень бойової техніки в режимі реального часу.
- *Аналіз даних* дозволить розробити географічні моделі, здійснювати їх комп'ютерне оброблення, досліджувати їх результати за методами машинного навчання. Подібний тип аналізу високоефективний при оцінці певних геолокацій і їх придатності для аналізу конкретних цілей, дозволяє прогнозувати результати та інтерпретувати відповідні зміни.
- *Картографування* забезпечить функціональну інтерпретацію даних, зокрема, візуалізації карт, що досягається можливістю у визначенні місця катастрофи. На даному етапі своєчасне виявлення загроз дозволить підвищити безпеку та систему захисту.
- *Візуалізація*, яка досягається за допомогою геолокаційних систем, здатна зменшити ризики катастроф. До прикладу, визначення вразливих районів за допомогою карт призводить до евакуацій та операцій з порятунку. Карти дозволяють визначити незахищені

або навпаки відносно безпечні ділянки, або забезпечення альтернативних маршрутів порятунку.

При функціонуванні віртуального інструменту, достатньо навести камеру смартфона на досліджуваний об'єкт та отримати результати в оцифрованому форматі. В подальшому, при картографуванні, можна буде обрати відповідний об'єкт/об'єкти на інтерактивній карті. Даний застосунок зможе використовувати датчики гаджетів (камеру, мікрофон, акселерометр і гіроскоп) для формування інтелектуальної бази, розпізнавання та навчання нейронної мережі на об'єктах техніки військового призначення, в якому кожен зможе додавати/спостерігати результати системи озброєнь засобами штучного інтелекту.

На даному етапі розробки важливим є запровадження власної інтелектуальної база даних еталонів за їх вхідними параметрами та точними коефіцієнтами, що реалізоване за методами машинного навчання, а саме:

- процесів сегментації зображень
- застосування порогових коефіцієнтів для ідентифікації шарів техніки військового призначення;
- розпізнавання образів використаної військової техніки за допомогою алгоритмів глибокого навчання;
- передруковування нейронною мережею растрових зображень;
- калібрування і зміни вхідних параметрів для нейронної мережі, доповнення бази даних більшою кількістю еталонів;
- перенавчання нейронної мережі за бажаною планіметричною точністю.

Найважливішим етапом стане процес *ідентифікації*. В межах сформованої бази даних, буде проводитись розпізнавання відомих марок та моделей БПЛА, цифрових відбитків безпілотників або контролера (при використанні комунікації Wi-Fi) за їх MAC-адресами, а радіолокатор детекції посилає радіосигнал та реєструє його відображення від об'єктів, визначаючи напрямок та їх положення. Дана можливість може надати велику цінність для судових розслідувань, оскільки це стає підтвердження того, що саме той або інший об'єкт військового призначення були активними у відповідні періоди.

Для громадського населення буде важливим донесення своєчасної інформації про наближення загрозливих об'єктів військового призначення та їх достовірне місцезнаходження, що значно підвищить персоналізовану ситуаційну інформативність та можливість розгортання заходів протидії.

Щоденні дані, які накопичуються та обробляються, мають критичний геопросторовий контекст місцезнаходження і часу, що, власне, є відповідним виміром геопросторових знань. Супутники, повітряні/мобільні/фіксовані/погодні та інші IoT-датчики є джерелами, які постійно надають/поновлюють дані в режимі реального часу.

Режими роботи застосунку для відстеження техніки військового призначення можуть бути *пасивними* (тільки для спостерігання/прослуховування/відстеження) або *активними* (надсилають тривожний сигнал/аналізують отриману інформацію/повідомляють заходи безпеки), а також має наступні можливості управління:

- детекція;
- класифікація або розпізнавання;
- пошук та відстеження;
- передбачення та сповіщення.

В даному мобільному застосунку створена технологія з використанням алгоритмів машинного навчання і штучного інтелекту для розпізнавання і класифікації техніки військового призначення на інтерактивних картах. Застосунок буде корисним для військових і правоохоронних служб під час виконання відповідних завдань. Крім цього, застосунок буде корисним і для цивільних громадян, щоб вони мали можливість пройти до сховищ або виконати необхідні заходити щодо їх безпеки. В майбутньому, планується створити єдину базу знань для військових, де різні підрозділи зможуть обмінюватись інформацією інноваційної техніки різного військового призначення країн світового альянсу.

к.т.н. Золотухіна О.А. (ДУТ)

ОРГАНІЗАЦІЯ ОНЛАЙН-ВЗАЄМОДІЇ З ВИКОРИСТАННЯМ МЕТОДІВ ФАСИЛІТАЦІЇ

Сучасні виклики процесів спілкування в освіті та бізнесі пов'язані зі значним зростанням частки онлайн форми взаємодії між учасниками комунікації. Не зважаючи на те, що традиційні асинхронні методи обміну робочими повідомленнями, завданнями, звітами, коментарями тощо з використанням, наприклад, електронної пошти, залишаються актуальними, вони не дозволяють повною мірою забезпечити своєчасне реагування на зміни в робочих чи навчальних процесах. При цьому, організація синхронної онлайн-комунікації за наявності навіть невеликої кількості учасників деякого заходу (від 3-5 осіб) призводить до того, що переважна більшість учасників не задіяна активно, а перетворюється на пасивних слухачів. Особливо це критично для освітньої сфери при проведенні онлайн практичних навчальних занять, семінарів тощо.

Задачу організації онлайн-взаємодії будемо розглядати на прикладі навчального заняття практичної спрямованості для невеликих (5-15 осіб) та середніх (16-40) розмірів груп. В якості програмних засобів взаємодії використовується платформа Zoom. Додатковими засобами, що забезпечують підтримку процесу онлайн-взаємодії, можуть виступати Google-документи, Google-таблиці тощо або спеціальні дошки для колективної роботи, створені, наприклад, за допомогою Miro, Trello, Mural чи інших подібних сервісів. Ці засоби дозволяють організувати доступ до підсумкового звіту та інших артефактів для спільної роботи команди. Для забезпечення швидкої комунікації може бути використано телеграм-чат, куди заздалегідь підключено всіх учасників процесу.

Мета дослідження полягає у забезпеченні ефективної онлайн-взаємодії під час навчального заняття за рахунок використання методів фасилітації.

Типова організація онлайн-взаємодії під час навчального заняття використовує архітектуру, представлену на рис.1. Ключовою проблемою при такій організації є те, що зі зростанням чисельності групи стає дуже складно здійснити перевірку виконаних завдань протягом заняття, тому цю активність доводиться виносити в асинхронний режим. Це значно збільшує витрати часу викладача.

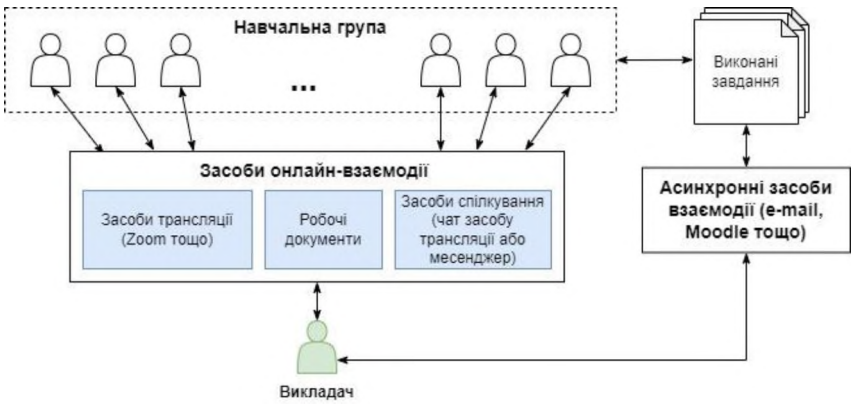


Рис. 1. Архітектура типової онлайн-взаємодії під час навчального заняття

Якщо під час заняття окремий студент демонструє результати виконання завдання, то складність становить контроль дій інших учасників групи, оскільки увага викладача зосереджена на одній роботі, крім того, інші учасники в цей момент не можуть одночасно повноцінно виконувати власне завдання та слідкувати за поясненнями викладача щодо можливих помилок у виконанні завдання. Якщо припустити, що заняття має тривалість 90 хвилин і на організаційні моменти та пояснення завдання викладач витратить принаймні 15 хвилин, а самий сильний студент в групі виконав завдання хоча б за 15 хвилин, то при

чисельності групи в 20 осіб на те, щоб кожен студент продемонстрував результати безпосередньо протягом заняття буде відведено (90-15-20)/20=2,75 хвилини. Це є катастрофічно малою кількістю часу як для демонстрації результату, так і для обговорення можливих помилок та зауважень до роботи. При цьому, студенти, що вже продемонстрували результати, фактично будуть не задіяні в занятті. Кількість зв'язків викладача з групою в процесі навчального заняття дорівнює чисельності групи.

Фасилітація – це спеціальні дії, спрямовані на організацію групової роботи. Фасилітатором, тобто людиною, яка організовує групу таким чином, щоб вона досягла певної мети, в навчальному занятті виступає викладач. Запропонована архітектура системи організації онлайн-взаємодії на основі методів фасилітації наведена на рис.2. В якості засобу онлайн-взаємодії використовується платформа Zoom, оскільки вона має функціонал створення паралельно функціонуючих незалежних «кімнат» з командами учасників.

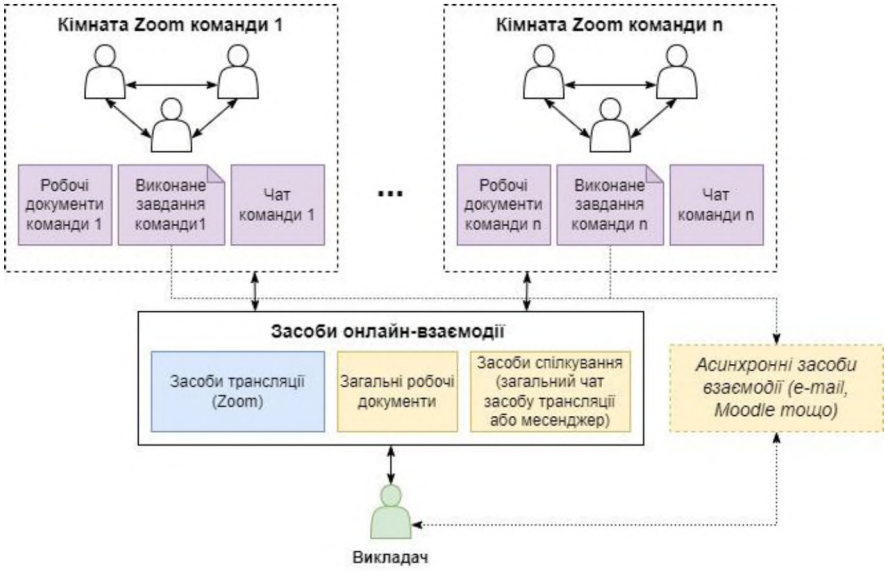


Рис.2. Архітектура онлайн-взаємодії на основі методів фасилітації

Для забезпечення ефективної онлайн-взаємодії навчальна група поділяється на команди по 3-5 осіб. Це дозволяє скоротити в 3-5 разів кількість зв'язків викладача протягом заняття. При цьому, в схему взаємодії додаються зв'язки між учасниками всередині команди і за рахунок невеликої чисельності команди вони забезпечують постійне залучення учасників до процесу виконання командного завдання протягом всього заняття. Завдяки використанню механізму кімнат Zoom, кожна команда має свій окремий робочий простір. Загальні робочі документи містять посилання на робочі простори кожної команди. При вказаній архітектурі, асинхронні засоби взаємодії не є основними інструментами для контролю виконання завдань. При таких же вхідних умовах розподілу часу на пояснення та виконання завдань (але для фасилітованого процесу паралельно працюють не окремі учасники, а команди), на демонстрацію результатів та їх обговорення залишається 55 хвилин. При чисельності групи в 20 осіб та поділі на 5 команд по 4 учасники можемо виділити по 10 хвилин на презентацію й обговорення результатів кожної команди, та 5 хвилин на заключне обговорення чи видачу домашнього завдання. Слід зазначити, що однією з умов процесу є презентація командою кінцевого готового рішення навчальної задачі безпосередньо під час заняття, що дозволяє викладачеві оцінити його в синхронному режимі взаємодії.

Таким чином, застосування методів фасилітації при організації онлайн-взаємодії під час навчального заняття дозволяє: забезпечити рівномірне та постійне залучення студентів до роботи протягом заняття; скоротити час викладача на перевірку завдань; оптимізувати зв'язки між учасниками впродовж онлайн-взаємодії за рахунок їх перерозподілу в командах.

к.т.н. Ільїнов М.Д. (ВІТІ ім. Героїв Крут)
Бочаров В.А. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЕЛЕКТРИЧНИХ ХАРАКТЕРИСТИК НАХИЛЕНОГО СИМЕТРИЧНОГО ВІБРАТОРА З КОМБІНОВАНИМ ПОЛОТНОМ ДЕКАМЕТРОВОГО ДІАПАЗОНУ

Радіозв'язок в декаметровому діапазоні відіграє важливу роль у військових (спеціальних) системах зв'язку. Це вид електрозв'язку, який надає користувачам можливість обмінюватися різними видами інформації на великі відстані (тисячі кілометрів) без ретрансляції сигналу через відбиття в іоносфері, а також без великих затрат енергії під час передачі радіосигналу.

В теперішний час, в сухопутних військах на заміну радіостанцій старого парку було прийнято на озброєння радіостанції виробництва компанії HARRIS. Однак антени які входять в поставку до цих радіостанцій не дуже добре себе зарекомендували, а саме їх невдалим технічним рішенням та високою вартістю. Відсутність якісних антен радіостанцій спричинило ряд труднощів при організації зв'язку в діапазоні коротких хвиль (КХ). Питання пов'язані з розробкою та модернізацією існуючих типів антен є актуальними і мають практичне значення. Ціль даної роботи аналіз електричних характеристик нахиленого симетричного вібратора з комбінованим полотном декаметрового діапазону.

З ціллю підвищення ефективності використання радіостанції нового покоління КХ діапазону пропонується ввести в склад антенно-фідерного приладдя полегшену телескопічну щоглу (ТЩ) висотою h ≈ 8-10м. Наявність ТЩ дозволяє розгорнути антену КХ діапазону для роботи на ближні та середні відстані між кореспондентами у вигляді симетричного нахиленого вібратора (ВН) з комбінованими плечима, ВН ($\frac{8(15,25)}{2}$) для роботи в діапазоні частот від 3 до 20 МГц. Антена має комбіноване полотно, виконане у вигляді трьох відрізків дроту, шляхом з'єднання яких можна створити довжину плеча 8, 15, 25 метрів (рис.1).

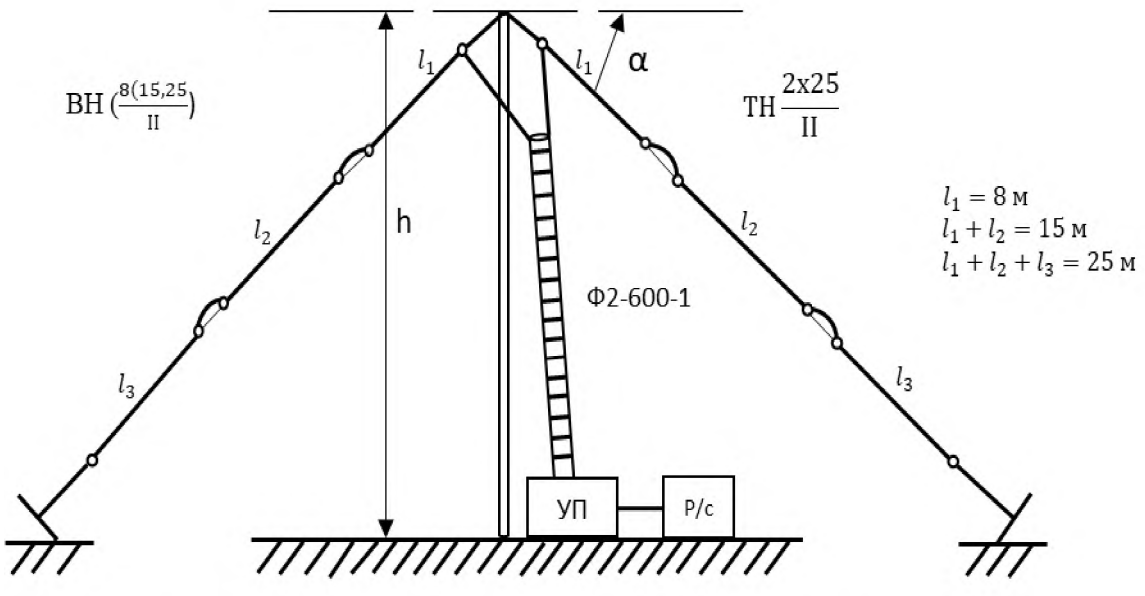


Рис.1. Технічне рішення антенно-фідерного пристрою

Пропонується живлення антени здійснити симетричним фідером типу Ф2-600-1 з використанням узгоджуючого пристрою (УП). Пристрій узгодження (антенний трансформатор), що дозволяє перетворити антену ВН ($\frac{2\times l}{h}$) для роботи з іоносферною хвилею, в нахилену Т – подібну антену (ТН $\frac{2\times l}{h}$), для роботи з земною хвилею.

Для аналізу характеристик ВН ($\frac{8(15,25)}{2}$), була застосована розрахункова модель у вигляді симетричного вібратора з висотою підвісу, яка визначається за формулою:

$h` = h - \frac{1}{2}\sin\alpha$,

де: $\alpha \approx 10\text{-}15^{\circ}$ - кут схилу плеча.

Антена забезпечує ефективну роботу просторової хвилі в трьох діапазонах частот: 2Δf1 = 3...6 [МГц], 2Δf2 = 6...12 [МГц], 2Δf2 = 12...24 [МГц],
а також, роботу земної хвилі (ЗХ), в діапазоні 2Δf1 = 3...6 [МГц] на антену з верхнім навантаженням.

В режимі роботи іоносферної хвилі (ІХ) характеристика направленості ВН ($\frac{2\times l}{h}$), з урахуванням нормальних параметрів землі ($\varepsilon' \neq 1,\ \sigma \neq \infty$) визначається виразом:

$$f_E(\theta) = \frac{\cos(kl\cos\theta) - \cos kl}{\sin\theta}\sqrt{1 + |R_В| - 2|R_В|\cos(2kh`\sin\theta - \Psi_В)}$$ – Е-площина, [1,2]

$$f_Г(\theta) = \sqrt{1 + |R_Г| - 2|R_Г|\cos(2kh`\sin\theta - \Psi_Г)}$$ – Н-площина,

де: $R_Г = |R_Г|^{j\Psi_Г} = \frac{\sin\theta - \sqrt{\varepsilon`_k - \cos^2\theta}}{\sin\theta + \sqrt{\varepsilon`_k - \cos^2\theta}}$ - …, $R_В = |R_В|^{j\Psi_Г} = \frac{\varepsilon`\sin\theta - \sqrt{\varepsilon`_k - \cos^2\theta}}{\varepsilon`\sin\theta + \sqrt{\varepsilon`_k - \cos^2\theta}}$ - коефіцієнти відбиття від землі, $\varepsilon'_k = \varepsilon` - i \cdot 60 \cdot \lambda \cdot \sigma$ – відносна комплексна діелектрична проникність Землі.

Для вертикальної площини, перпендикулярної осі вібратора (Н-площина) коефіцієнт направленості (D) визначається виразом:

$$D = \frac{480}{R\Sigma п}\sin\frac{kl}{2}\{1 + |R_Г| + 2|R_Г|\cos(2kh\sin\theta + \Psi_Г)\},$$

де: $R\Sigma п$ – опір випромінювання вібратора в опуклості з урахуванням впливу Землі.

Аналіз електричних характеристик широкосмугової антени ВН ($\frac{2\times l}{h}$) в режимі роботи ІХ показує, що параметри Землі майже не здійснюють впливу на форму діаграми направленості в двох ортогональних площинах, але втрати при відбитті поля від Землі позначаються на коефіцієнті направленої дії антени, так при ідеальній поверхні Землі (σ = ∞), D = 4.87 дБ, а при ε`= 4, σ = 10^{-3} (сухий ґрунт), D = 4 дБ в максимальному випромінюванні.

Таким чином, запропоноване компонування ВН ($\frac{8(15,25)}{2}$) з симетричним фідером, для роботи в складі радіостанцій нового покоління, дозволяє забезпечити роботою в широкому діапазоні, частотою на ближні та середні дальності просторовою хвилею, а також роботу зенітної хвилі на 50-100 км.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петров Б. М. Электродинамика и распространение радиоволн: Учебник для вузов. - 2-е изд., - М.: Горячая линия - Телеком, 2007. - 558 с.

2. Карл Ротхаммель. Антенны: Том 1. - 11-е издание, исправленное -Штутгарт, 1995. 415 с.

к.т.н. Ільїнов М.Д. (ВІТІ ім.Героїв Крут)
Булковський В.І. (ВІТІ ім. Героїв Крут)

РОЗРАХУНКОВА МОДЕЛЬ ЗИГЗАГОПОДІБНОЇ АНТЕНИ ДЛЯ АНАЛІЗУ ЗОВНІШНИХ ХАРАКТЕРИСТИК

Антени вібраторного типу знайшли найбільш широке застосування в діапазоні метрових, дециметрових і в нижній частині антени, сантиметрових хвиль, як самостійна антена, як елемент антенної решітки, як опромінювачі дзеркальних антен. Пріоритетне місце серед антен цього типу займають зигзагоподібні антени (ЗА), відрізняючись зовнішнім коефіцієнтом підсилення, роботою в широкому діапазоні частот з коефіцієнтом перекриття ($К_п$) =2...2,5, надійністю в роботі, механічною міцністю. Томупитання пов'язаних з розробкою ЗА, їх модернізацією є актуальним і мають практичну значимість на сьогоднішній день.

Одне із направлень розвитку ЗА є модернізація їх конструкцій, що дозволяють розширити не тільки функціональні можливості, але і покращити їх електричних характеристик зокрема розширити діапазонні можливості.

Конструкції багатодіапазонних ЗА, які дозволяють забезпечити роботу в діапазоні частот з $К_п$=4,а також в збільшенніG-коефіцієнта підсилення в області високих частот, показані на рис. 1.

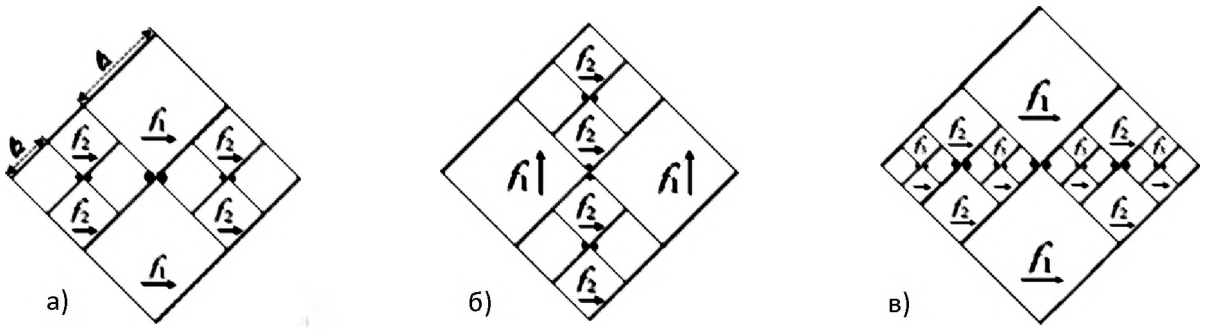


Рис.1.Багатодіапазонні зигзагоподібні антени: а)двохдіапазонна з горизонтальною поляризацією, б)двохдіапазонна з вертикальною поляризацією, в)трьохдіапазонна з горизонтальною поляризацією

В даному дослідженні представлений теоретичний аналіз електричних характеристик двохдіапазонної ЗА, показаний на рис.1(а). Була розроблена розрахункова модель ЗА з екраном для аналізу зовнішніх характеристик таких випромінювачів. Характеристика направленості в діапазоні нижніх частот (f_1) має наступний вигляд[1,2]:

$$\psi(\theta,\varphi) := \left| \frac{1}{N} \cdot \left(\frac{\cos kl \cdot \sin\theta \cdot \sin\varphi - \cos kl}{\sqrt{1-\sin\theta^2 \cdot \sin\varphi^2}} \cdot \sin kh \cdot \cos\theta \cdot \frac{\sin\frac{N \cdot kd \cdot \sin\theta \cdot \cos\varphi}{2}}{\sin\frac{kd \cdot \sin\theta \cdot \cos\varphi}{2}} \right) \right|$$

де: N-кількість випромінювачів розрахункової моделі у вигляді симетричних вібраторів;

h-висота антени над екраном;

d-відстань між випромінювачами.

Розрахунок характеристики направленості в смузі верхніх частот (f_2) проводиться згідно виразу, який відрізняється від попередньої формули множником антенної решітки[3]:

$$\psi(\theta,\varphi) := \left| \frac{1}{N} \cdot \left(\frac{\cos kl \cdot \sin\theta \cdot \sin\varphi - \cos kl}{\sqrt{1-\sin\theta^2 \cdot \sin\varphi^2}} \cdot \sin kh \cdot \cos\theta \cdot \frac{\sin\frac{N \cdot kd \cdot \sin\theta \cdot \cos\varphi}{2}}{\sin\frac{kd \cdot \sin\theta \cdot \cos\varphi}{2}} \cdot \frac{\sin kd1 \cdot \sin\theta \cdot \cos\varphi}{\sin\frac{kd1 \cdot \sin\theta \cdot \cos\varphi}{2}} \right) \right|$$

Результати теоретичного аналізу показані на рис. 2, де представлені діаграми направленості в двох ортогональних площинах для різних смуг частот[4].

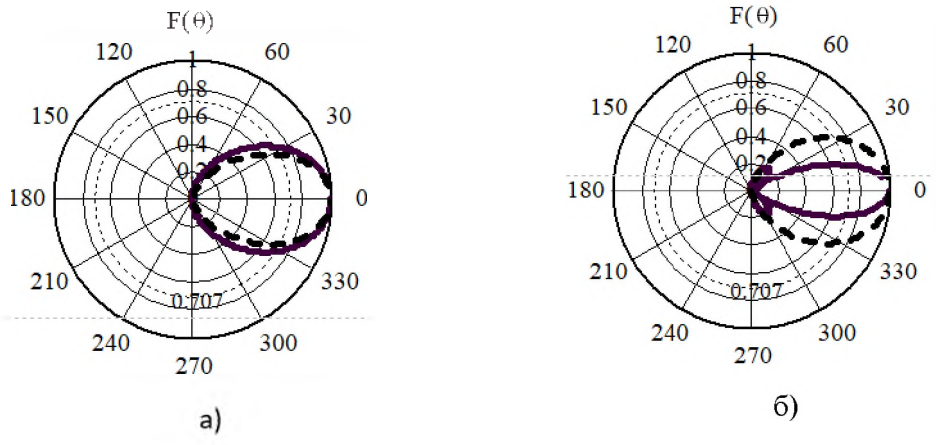


Рис. 2. Діаграми направленості двохдіапазонної зигзагоподібної антени в двох смугах робочих частот: а) область низьких частот, б) область високих частот

Результати розрахунку наглядно показують працездатність запропонованого технічного рішення по компоновці ЗА, а також збільшення коефіцієнта підсилення в області високих частот.

В області низьких частот (f_1) при довжині плеча 0,25λ коефіцієнт підсилення дорівнює приблизно G = 7.8 dBi, а в області високих частот (f_2) коефіцієнт підсилення дорівнює G = 10 dBi.

Таким чином, проведені розрахунки наглядно показують великі функціональні можливості багатодіапазонних зигзагоподібних випромінювачів. Такі антени дозволяють збільшити смугу робочих частот в 4-5 разів (рис. 1 а,б.), а також підвищити коефіцієнт підсилення в області високих частот на 1,5…2,5 dBi. Пропоноване технічне рішення по компоновці зигзагоподібних антен надійні в роботі, мобільні, дозволяють збільшити розвідзахищеність, що особливо важливо при застосуванні в бойових умовах на сьогоднішній день.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D. Sengupta, "The radiation characteristics of a Zig-Zag antenna", IRE Transactions on Antennas and Propagation, vol. 6, pp. 191-194, 1958.

2.Сомов А.М. Проектирование антенн / А.М. Сомов, Р.В. Кабетов. – М.: Горячая линия–Телеком, 2015. С. 126-138.

3. C. A. Balanis, "Antenna Theory analysis and design", John Wiley and Sons, Inc., 3rd ed., 2005.Pp. 68-82.

4. Харченко К. Зигзагообразная антенна. - Радио, 1961, № 3. С. 28-30; 1999, № 8. С. 17.

к.т.н. Ільїнов М.Д. (ВІТІ ім. Героїв Крут)
Козуб Д.С. (ВІТІ ім. Героїв Крут)

ШИРОКОСМУГОВА ОДНОДЗЕРКАЛЬНА ПАРАБОЛІЧНА АНТЕНА

Розробка широкодіапазонних дзеркальних антен (ДА) та дослідження їх характеристик, є одним із направлень розвитку антенної техніки яка працює в діапазоні ультра коротких хвиль.

Такі антенні пристрої, дозволяють не тільки підняти енергетичний потенціал радіолінії, а ще й розширити функціональні можливості радіосистеми в цілому.

Одним із важливих елементів дзеркальної антени, є первинне джерело електромагнітного поля – опромінювач, який визначає характеристики антени, у тому числі і можливості її роботи в заданому діапазоні частот.

В даній роботі, пропонується у якості опромінювача ДА, використовувати логоперіодичну антену (ЛПА) вібраторного типу, яка забезпечує роботу в діапазоні частот з коефіцієнтом перекриття ($К_П$) ≈ 10. Такий опромінювач компактний, має мінімальний затіняючий ефект, не потребує додаткових елементів для кріплення до дзеркала параболічної антени.

Зовнішні характеристики ЛПА в 2-х ортогональних площинах визначаються за формулою:

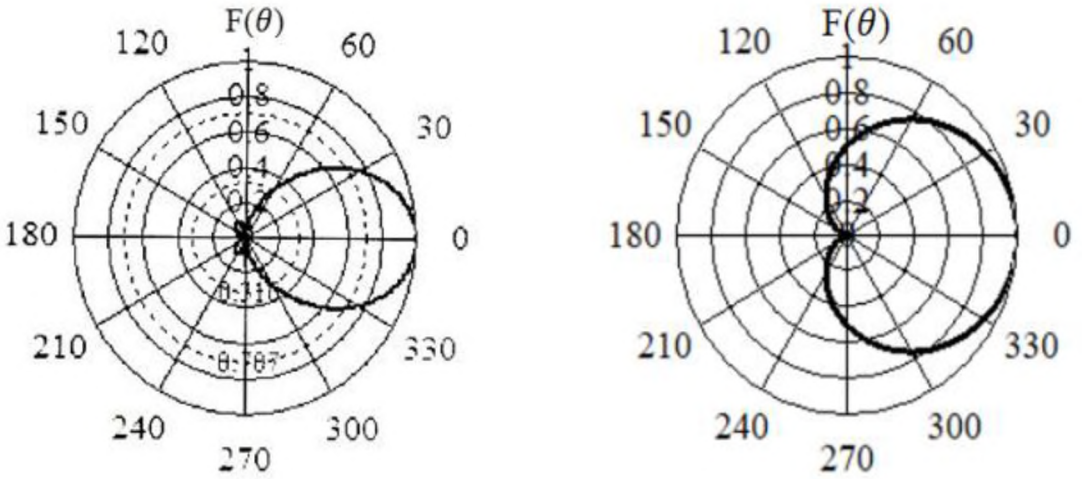
$$F^E(\theta) = \frac{\cos\left(\frac{\pi}{2}\sin(\theta)\right)}{\cos(\theta)} \cdot sin\left[\frac{\pi}{4}\cdot(1-\tau)\cdot \operatorname{acos}(\alpha)\cdot(1+\cos(\theta))\right], ,$$

$$F^H(\theta) := \left|\sin\left(\frac{\pi}{4}\right)\cdot(1-\tau)\cdot\cot(\alpha)\cdot(1+\cos(\theta))\right|,$$

де: τ – період структури ЛПА;

α - половина кута структури.

Діаграми направленості (ДН) ЛПА вібраторного типу зображені на рис. 1. Отриманий результат наглядно показує один із важливих недоліків ЛПА як опромінювача ДА – несиметрична ДН в двох ортогональних площинах.



а) б)

Рис. 1. ДН ЛПА в двох ортогональних площинах:
а) Е – площина, б) Н – площина

Розміри усіченого параболоїда (рис. 2) визначається шириною ДН опромінювача в двох ортогональних площинах, відповідно до виразу:

$$2R_{01} \approx 75\frac{\lambda}{2\Delta\theta^{H}_{0.1}};\ 2R_{02} \approx 75\frac{\lambda}{2\Delta\theta^{E}_{0.1}},$$

де: $2\Delta\theta^{H}_{0.1}$– ширина ДН опромінювача (ЛПА) в площині Н, по рівню 0,1 від максимума потужності випромінювання;

$2\Delta\theta^{E}_{0.1}$ – ширина ДН опромінювача (ЛПА) в площині Е, по рівню 0,1 від максимума потужності випромінювання.

Кут розкриву $(2\psi_{02})$ дзеркала в ортогональних площинах, визначається виразом:

$$2\psi_{01} \approx 2\Delta\theta^{H}_{0.1} \text{ та } 2\psi_{02} \approx 2\Delta\theta^{H}_{0.1}.$$

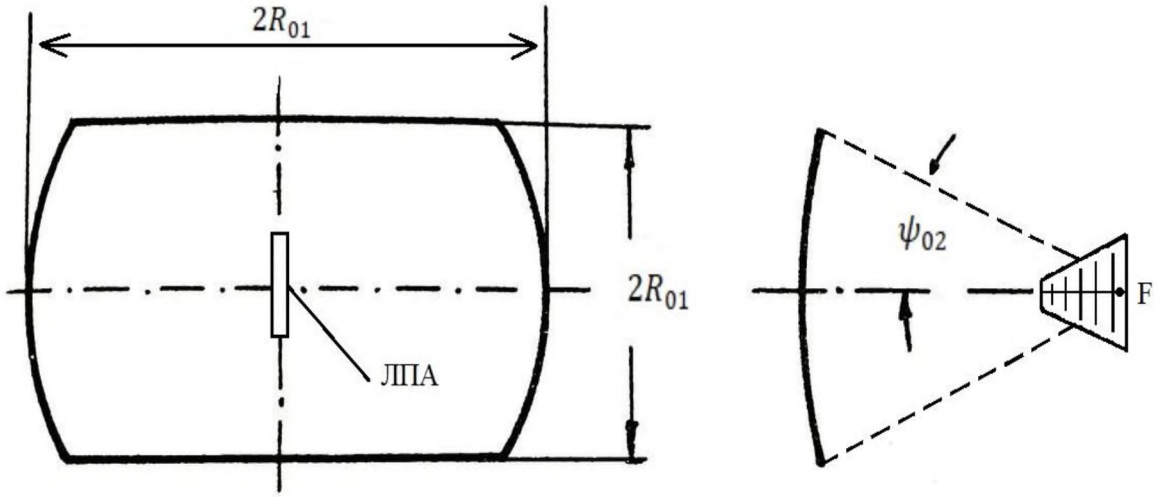


Рис. 2. Геометрія симетричного усіченого параболоїда

Таким чином, запропоноване технічне рішення з компонування ДА, дозволяє забезпечити роботу у широкому діапазоні робочих частот з $К_{П} \approx 10$, за рахунок використання опромінювача у вигляді плоскої ЛПА вібраторного типу. Така антена відрізняється простотою конструкції, не потребує додаткових елементів кріплення опромінювача до дзеркала, та має мінімальний затіняючий ефект.

Антену можна використовувати для радіорелейного зв'язку, бездротової прив'язки робочого місця, для передачі даних по Wi-Fi мережі, а також для збільшення розвідзахищеності і підвищення надійності роботи системи в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Логопериодические вибраторные антенны: Учебное пособие для вузов / [Петров Б.М., Костромитин Г. И., Горемыкин Е.В.] М.: Горячая линия – Телеком, 2005. – 239с.: ил.

2. Designing of Log Periodic Antennas: A Computational Approach / [Deepak Sharma]. U.: LAP LAMBERT Academic Publishing, 2012. - 68 p.

Калашніков І.А. (ТОВ «Радіо Сатком Груп»)

МЕРЕЖІ ОПОВІЩЕННЯ З ВИКОРИСТАННЯМ УКХ РАДІОСТАНЦІЙ HARRIS RF-7800V ТА RF-7850M

Сучасна війна яскраво показала необхідність і важливість наявності мереж оповіщення підрозділів. Трапляється дуже багато випадків, коли необхідна інформація доводиться вже після того, як перестала бути актуальною, через те, що немає єдиної мережі оповіщення підпорядкованих та взаємодіючих підрозділів.

Мережі оповіщення мають бути малопомітними для технічних засобів противника, але здатними при цьому оперативно передавати важливу інформацію. Також дуже важливою вимогою є простота їх розгортання та експлуатації. Мережі оповіщення мають забезпечити доведення інформації як на стаціонарні пункти управління, так і на пункти управління, розгорнуті на рухомих об'єктах.

Щоб задовільнити ці вимоги наявності самих лише засобів радіозв'язку недостатньо, адже взаємодіючі підрозділи можуть розташовуватись на великих відстанях один від одного, а розширення зони покриття шляхом розташування антенно-фідерних пристроїв на більш вигідних локаціях і збільшення потужності передавача може призвести до виявлення противником таких радіомереж з подальшим впливом на них. Також не виключено перебування абонентів в "мертвих зонах" або поза межами прямої видимості, що є поширеною проблемою.

Використання телефонних мереж з метою оповіщення підрозділів також не завжди задовольняє всі вимоги, адже телефонні мережі не забезпечують оперативність під час оповіщенння низки підрозділів.

Функціонал сімейства радіостанцій HARRIS RF-7800V та RF-7850M є яскравим прикладом вирішення проблем в розгортанні та функціонуванні мереж оповіщення сукупно з іншим мережевим обладнанням.

За допомогою функції Retransmit, яка підтримується радіостанціями RF-7800V та RF-7850M є можливість організувати обмін голосом між радіостанціями різних радіомереж за допомогою IP-мереж. Функція Retransmit доступна для всіх режимів роботи радіостанцій. У разі відповідних налаштувань весь трафік може шифруватися за допомогою алгоритмів шифрування AES або CITADEL з довжиною ключів 128 або 256 біт.

За допомогою режиму роботи CWR, який також є однією з функцій радіостанцій RF-7800V та RF-7850M, є можливість організувати мережі обміну голосом і даними як в межах прямої видимості з використанням локальних ретрансляторів або без них, так і поза її межами за допомогою IP-мереж. У разі відповідних налаштувань голос і дані можуть шифруватися за допомогою алгоритмів шифрування AES або CITADEL з довжиною ключів 128 або 256 біт. Службові дані в IP-мережах додатково шифруються ключем 64-hex.

Завдяки функції Retransmit та режиму роботи CWR можливо розгорнути мережі оповіщення за допомогою малопотужних радіостанцій, що мінімізує можливість їх виявлення та впливу технічних засобів противника на мережі, але забезпечує при цьому доведення необхідної інформації усім абонентам.

Налаштування функції Retransmit або режиму роботи CWR не потребує багато часу і не є складним процесом. Більш детальна інформація про функціонал наведена в інструкціях з експлуатації радіостанцій. Супутнє мережеве обладнання, необхідне для функціонування мереж, є доволі розповсюдженим в підрозділах Збройних Сил України, що значно полегшує розгортання мереж оповіщення і зазвичай не потребує додаткових вкладень.

Функціональні можливості радіостанцій RF-7800V та RF-7850M здатні задовольнити сучасні вимоги до функціонування мереж оповіщення підроздлів, які є дуже важливим елементом системи управління.

Кирилюк Д.О. (ЖВІ ім. С.П. Корольова)
Папуш О.Г. (ЖВІ ім. С.П. Корольова)

ВИТІК КОНФІДЕНЦІЙНОЇ (ОСОБИСТОЇ) ІНФОРМАЦІЇ ТА ЇЇ ВИКОРИСТАННЯ ЗЛОВМИСНИКАМИ.

В даний час тема збереження інформації найбільш актуальна. Ми маємо берегти свої особисті дані, щоб не допустити їх витік та використання зловмисниками. Наразі відбувається найбільший відсоток злочинів, пов'язаних з витоком конфіденційної (особистої) інформації. Шахраї користуються неосвіченістю громадян, а також йде збір необхідних даних щодо того чи іншого об'єкту, по якому може поцілити ворог. Тож маємо своє бачення щодо вирішення даної проблеми.

Щоб уникнути витоку інформації, необхідно дотримуватись деяких правил:

1. Захист особистих акаунтів. Для вирішення проблеми в даній сфері нам необхідно використовувати двофакторну аутентифікацію, яка полягає в тому, що для того щоб отримати доступ до особистої сторінки користувач має пройти декілька етапів ідентифікації, та підтвердження особистості, для того, щоб забезпечити більш стійкий захист від злому особистих даних. Також для запобігання підбору паролю дуже важливим моментом є встановлення складних паролів, що будуть змінюватися якомога частіше. Важливо: заборонено використовувати однакові паролі для своїх акаунтів в різних соціальних мережах.

2. Контент, який публікується. В обов'язковому порядку прибирати геовідмітку з фотографій та інших публікацій, які потрапляють на сторінку. Необхідно слідкувати за фоном світлин: вивіски, номери машин, відомі об'єкти, які видають локацію. Бо саме через свою необережність великий відсоток користувачів допускають виток інформації за допомогою якої в подальшому ворог може складати приблизну карту місцевості та наносити удари.

3. Взаємодія з іншими користувачами. Якомога менше вказувати родичів та інформацію про них. Як приклад, можна знайти за доступною інформацією акаунт матері, де вказано її дівоче прізвище. А це у 96% випадків кодове слово в банку, за допомогою якого злочинці можуть з легкістю отримати доступ до банківського рахунку людини.

4. Однією з найбільш поширених проблем сучасного світу (стосовно Інтернет мереж) є фішинг та інше шахрайство. Ні в якому разі не надавати дані, які можуть бути використані підозрілими особами або сайтами. Наприклад, якщо ви не брали участі в лотереї, а вам приходить про це сповіщення, або ж надходить телефонний виклик, то вказувати номер картки або ж диктувати останні цифри чи код, який надходить на ваш номер телефону, щоб отримати 100 тисяч гривень виграшу, не потрібно. Це збереже вас від втрати грошей, а також від надавання доступу до своїх особистих даних шахраям.

5. Слід обережно поводитися з спливаючими вікнами і посиланнями. Якщо ви при перегляді вебсторінок потрапляєте на підозрілі посилання, ні в якому разі не переходити за ними. В кращому випадку необхідно одразу закривати всі підозрілі (невідомі) посилання і реклами.

6. Слідкуйте за розмовами, що ведете. В сучасному світі виникає проблема прослуховування мобільних телефонів. Ви могли неодноразово це помічати, коли ведеться розмова за покупку, або ж місця відпочинку, а через деякий час на вашому телефоні спливає реклама з пропозицією того, про що велась ваша розмова. Тож щоб запобігти даній проблемі, маємо декілька шляхів вирішення: менше говорити на конфіденційні теми, які не мають з'явитися в соціальних мережах, або ж здійснити переналаштування телефону, яке буде запобігати прослуховуванню і витоку особистої інформації.

Висновок: для збереження в безпеці своїх особистих даних ми маємо дотримуватися описаних правил, які в подальшому захистять нас від ситуацій, з яких вже неможливо знайти вихід, а також щоб не допустити витоку інформації, яка може завдати шкоди, при потраплянні до рук зловмисників і шахраїв.

к.т.н. Козубцова Л.М. (ВІТІ ім. Героїв Крут)
к.т.н. Бескровний О.І. (ВІТІ ім. Героїв Крут)
д.п.н., к.т.н. Козубцов І.М. (ВІТІ ім. Героїв Крут)

ГІБРИДНА ПОБУДОВА СИСТЕМИ КІБЕРБЕЗПЕКИ НА ЗАСАДАХ ВІЙСЬКОВО-ЦИВІЛЬНОГО СПІВРОБІТНИЦТВА

З початком повномасштабної військової агресії Російської Федерації проти України, Державні органи та формування сектору безпеки і оборони України зіткнулися з веденням гібридної війни проти себе із застосуванням кіберпростору. Порушення функціонування українського сегменту кіберпростору змусило переглянути існуючі підходи до побудова системи кібербезпеки і таким чином забезпечити гарантовану безпеку держави.

Аналіз досліджень показав, що дана проблематика привернула увагу зарубіжних та вітчизняних науковців, однак предмет їх дослідження не охопив питання функціонування кіберпростору Державних органів та формування сектору безпеки і оборони України в умовах гібридної війни.

Мета доповіді. Обґрунтувати підстави створення гібридної системи кібербезпеки Державних органів та формування сектору безпеки і оборони України на засадах військово-цивільного співробітництва. Для досягнення мети поставлено такі задачі: 1. Проаналізувати сучасний стан досліджень та публікацій. 2. Обґрунтувати підстави створення гібридної системи кібербезпеки Державних органів та формування сектору безпеки і оборони України на засадах військово-цивільного співробітництва.

3. Обговорити адміністративно-правові засади гібридного військово-цивільного співробітництва Державних органів та формування сектору безпеки і оборони України.

Результати дослідження. Пропонується можливість організувати функціонування та взаємодію Державних органів та формування сектору безпеки і оборони України з приватним сектором для нейтралізації кіберзагроз на підставі Статті 10. «Державно-приватна взаємодія у сфері кібербезпеки» Закону України «Про основні засади забезпечення кібербезпеки України», де визначено:

пункт 1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

підпункт 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

підпункт 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

підпункт 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

підпункт 6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

підпункт 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Враховуючи вище зазначене, небайдужими адміністраторами було створено телеграм-канал «Кібер Армія», «Stop Russian Channel MRIYA». До професіоналів сфери ІТ долучилось понад 250 тисяч активних учасників звичайних людей для активних дій у кіберпросторі. Адміністратори періодично і за результатами обстановки в кіберпросторі формували дозовані завдання небайдужими фахівцями в галузі ІТ та кібербезпеки, а саме блокування інтернет ресурсів, що поширювали інформацію про насилля, шляхом подачі відповідних заявок адміністраторам відповідних ресурсів; реалізація активних заходів впливу на порушення правильності функціонування об'єктів критичної інформаційної інфраструктури РФ та Республіки Білорусь.

Таким чином, високу ефективність у протистояння гібридній війні РФ та нейтралізації кіберзагроз Державним органам та формуванням сектору безпеки і оборони України проявили саморганізовані гібридні підрозділи військо-цивільного співробітництва.

Кокошинський В.В. (ВІТІ ім. Героїв Крут)
Краснобокий А.В. (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ МЕРЕЖ SDN У ВІТЧИЗНЯНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Важливою тенденцією в розвитку сучасних телекомунікаційних систем та мереж є впровадження програмно-конфігурованих рішень.

Основна ідея програмно-конфігурованих мереж (англ. software-defined networking, SDN) полягає в розділенні функцій управління мережею та функцій передачі даних, і програмній реалізації.

Тобто на відміну від традиційної мережі, в якій маршрутизація – це розподілений процес, при якому топологія мережі розраховується сумісно усіма пристроями, в SDN – це програма моделювання мережі з заданими параметрами.

Навчившись успішно віртуалізувати обчислювальні ресурси, IT-галузь витратила чимало часу на пошук адекватного підходу для віртуалізації мереж, мережевих сервісів та розподілених систем зберігання даних. Традиційний стек протоколів не пропонував потрібного рішення ні для гнучкого управління розподілом мережевих ресурсів і якістю мережевих сервісів, ні для динамічного перерозподілу даних, що зберігаються в рознесених системах зберігання даних. Прорив намітився саме з появою концепції SDN.

Традиційні телекомунікаційні мережі проектувалися з розрахунку на використання спеціалізованих апаратних пристроїв (маршрутизаторів, комутаторів, міжмережевих екранів, та ін.), які створювалися на базі специфічних апаратних та програмних платформ окремих вендорів.

Проектування та розгортання мереж, побудованих на таких «монолітних» мережевих елементах призводило до досить тривалих циклів пусконалагоджувальних робіт, негнучкості та дорожнечі мережі, а, отже, і до уповільнення виведення на ринок нових продуктів та послуг. Обслуговування та управління такою мережею було також досить неефективним та дорогим.

За рахунок введення програмованості та абстрагування функцій мережі концепція SDN змінила самі принципи побудови мереж. Абстрагування полягає у відокремленні функцій від структури та топології, а також поділ функціоналу за ієрархією рівнів.

Централізації площини управління на єдиному SDN-контролері знижує кількість операцій управління, полегшує їх і дає можливість оркестрації ресурсів та сервісів. Крім того, SDN дозволяє ввести стандартні протоколи та моделі даних, а це, в свою чергу, дозволяє здійснювати централізоване управління в гетерогенній (побудованій на обладнанні різних вендорів) та багаторівневій мережі.

Технологія SDN забезпечує абстрагування топології мережі та моделей даних для вищих систем. Це дає можливість швидкого введення нових програм, заснованих на властивості програмованості мережі.

Побудова програмно-конфігурованих мереж з урахуванням технології SDN дає такі переваги, які у традиційних архітектурах відсутні або їх використання значно збільшує вартість володіння інфраструктурою:

повна програмованість мережі за рахунок відокремлення рівня управління трафіком від рівня передачі даних та перенесення функцій управління на виділені обчислювальні ресурси;

максимально ефективне використання пропускної спроможності мережного обладнання шляхом оптимізації пересилання мережевих потоків;

створення ізольованих віртуальних мереж для кожного клієнта IT-послуг на базі єдиної фізичної інфраструктури;

динамічне підстроювання ємності віртуальної мережі та інших параметрів під потреби клієнта, що зростають, без зміни фізичної топології;

масштабованість, що забезпечує збільшення числа логічних мереж без зниження продуктивності вже існуючих віртуальних конфігурацій;

підвищення безпеки за рахунок "наскрізного" управління захисними політиками в кожному мережевому пристрої для окремих потоків;

збільшення надійності функціонування мережі за допомогою централізованого керування конфігурацією мережевих параметрів на рівні сесій, користувачів, пристроїв та програм.

Серед основних недоліків використання технології SDN слід зазначити те, що контролер є вузьким місцем роботи мережі, тому надійність та продуктивність роботи мережі будуть в першу чергу залежати від надійності та продуктивності роботи контролера. Масштабованість мережі також буде залежати в першу чергу від потужності контролера, до якого буде надходити більше трафіку від зростаючої кількості комутаторів.

Крім того, для здійснення переходу на SDN необхідно:

змінити всю інфраструктуру для реалізації протоколу SDN і контролера SDN, тобто, потрібна повна реконфігурація мережі;

підвищити кваліфікацію персоналу.

Отже, виникнення концепції SDN виводить три основні складові ІТС (сервери, системи зберігання та мережі) на єдиний рівень з точки зору віртуалізації, що в перспективі значно покращує показники мобільності, продуктивності, керованості якістю та дозволяє створити єдиний віртуальний простір вітчизняних телекомунікаційних систем і мереж.

На даний час реалізація концепції SDN дозволила суспільству «піднятись» над рівнем суто фізичної апаратної побудови телекомунікаційних систем і мереж, позбувшись тягарю дорогих мережевих пристроїв з їх складністю модернізації та прив'язки до конкретного виробника, що полегшує удосконалення та подальше обслуговування вітчизняних телекомунікаційних систем і мереж.

Незважаючи на те, що відсутність стандартів для повного контролю пристроїв поки що перешкоджає широкому впровадженню технологій SDN, фахівці прогнозують щорічне збільшення ринку SDN в середньому на 25% найближчі роки. А отже, для нашої країни, яка буде швидкими темпами відновлювати та покращувати власну обороноздатність після відбиття ворожої агресії та за підтримки західних партнерів, є нагальна потреба впроваджувати найбільш передові технології, серед яких є застосування технології SDN у вітчизняних телекомунікаційних системах і мережах.

Отже, SDN – це фундамент, з якого, за дослідженням фахівців, і було б зручно починати будівництво телекомунікаційних систем та мереж при їх виникненні. Завдяки відкритому коду та перспективності застосування розвиток технологій SDN широко підтримується провідними спеціалістами ІТ галузі.

Концепція SDN продовжує активно досліджуватись, знаходячи свій подальший розвиток, зокрема, в технологіях SD-WAN і NDN, та впроваджуватись в різних напрямах екосистеми інформаційно-комунікаційних технологій, таких як хмарні технології, засоби штучного інтелекту, аналітика великих даних та застосування Інтернету речей.

Колесник О.С.(ДУТ)
к.ф.-м.н Поперешняк С.В. (ДУТ)

ВІДОБРАЖЕННЯ ПУХЛИН ГОЛОВНОГО МОЗКУ НА ОСНОВІ МЕТОДІВ СЕГМЕНТАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ

Актуальність

Розпізнавання тих локацій головного мозку, де виникають аномалії на цифрових зображеннях, зокрема МРТ, комп'ютерною системою грає велике значення для полегшення роботи медичних закладів, адже спрощує процес виявлення непомітних ореолів пухлин на початковому етапі хвороби, коли людське око майже не здатне відрізнити невеликі відмінності у кольорах.

Оскільки обробка даних магнітного резонансу спеціалістами є доволі трудомістким завданням, то розробка методів автоматичної сегментації пухлин головного мозку залишається одним із пріоритетних та найскладніших завдань обробки медичних даних.

Постановка задачі

1. Дослідити методи сегментації зображень МРТ головного мозку;
2. Розробити алгоритм сегментації цифрового зображення МРТ головного мозку з використанням методів комп'ютерного зору.

Мета

Поліпшити ручний або напівавтоматичний аналіз МРТ головного мозку за рахунок автоматичної обробки з використанням методів комп'ютерного зору.

Основні положення

Запропонований метод складається з трьох кроків:

1. Посилення контрастності цифрового зображення шляхом зміни масштабу зображення;
2. Видалення черепу із зображення для подальшої обробки зображення;
3. Сегментація пухлини.

У алгоритмі використовуються декілька добре відомих методів комп'ютерного зору: суміш Гауса, морфологічні операції та морфологічна реконструкція в градаціях сірого, порогове значення та алгоритм розрізання графа.

Розподіл суміші Гауса — це багатовимірний розподіл, який складається із суміші одного або кількох компонентів багатовимірного розподілу Гаусса. Кількість компонентів фіксується як вхідний параметр. Кожен багатовимірний компонент Гауса визначається його середнім і коваріацією, а суміш визначається вектором пропорцій змішування.

Морфологія вивчає форму. Математична морфологія здебільшого займається математичною теорією опису форм за допомогою множин. В обробці зображень математична морфологія використовується для дослідження взаємодії між зображенням і певним вибраним структурним елементом за допомогою основних операцій ерозії та розширення. У даному алгоритмі використовуються базові операції, такі як відкриття та закриття, а також більш складні морфологічні операції.

Морфологічна реконструкція відтінків сірого є ітеративним процесом. Вхідними для алгоритму є зображення маски. Фактично зображення маски є обробленим зображенням. У базовій морфологічній реконструкції для маркерного зображення застосовується бінарне розширення або ерозія. Потім алгоритм обчислює перетин із зображенням маски. Обробка триває до тих пір, поки значення зображення маски не перестануть змінюватися. Морфологічна реконструкція відтінків сірого базується на схожих принципах. Однак бінарне розширення або ерозію замінюється розширенням або ерозією відтінків сірого, а перетин замінюється вибором мінімального значення серед наборів точок.

Порогове значення є одним із найпростіших методів сегментації. Базовий метод замінює кожен піксель $P_{i,j}$ зображення на чорний або білий піксель відповідно до інтенсивності I пікселя. Вхідне порогове значення є фіксованою константою, яка називається порогом. Якщо $P'_{i,j}$ є пороговою версією $P_{i,j}$ відповідно до інтенсивності $I(P_{i,j})$, а T є пороговою, то:

$$P'_{i,j} = \begin{cases} 1 \text{ якщо } I(P_{i,j}) \geq T \\ 0 \text{ в іншому випадку} \end{cases}$$

У медицині , сегментація за порогом часто не вдається, оскільки медичні зображення мають дуже складний розподіл інтенсивності. Однак за пороговими методами часто слідують інші методи сегментації або поєднуються з іншими методами. Порогове значення в даному методі отримується за допомогою методу суміші Гауса.

Методи розбиття графів ефективні для сегментації. Вони моделюють зображення як зважений граф. У цьому алгоритмі пікселі пов'язані з вузлами. З'єднання між ними створюють зважені ребра. Значення вагових коефіцієнтів залежать від подібності або відмінності між сусідніми пікселями. Розріз графа — це спосіб розділити один граф на дві області відповідно до певних характеристик. Ребра, створені між двома розділами графа, називаються зрізаними ребрами. Вони мають ваги залежно від значень ваги країв між пікселями. Результуюча вага розрізу є сумою ваг розрізаних країв. Нарешті, результатом є набір розділів, і кожен розділ є сегментом зображення.

Алгоритм ітеративно сегментує передній план за допомогою моделі суміші Гауса. Отриманий розподіл пікселів використовується для побудови графа. Вузли у графові є пікселями, і два наступних наведених вузла додаються: вихідний вузол як S і приймальний вузол як T. Кожен піксель на передньому плані з'єднаний із S-вузлом, а кожен піксель на фоні – з T-вузлом. Вага ребер, які з'єднують пікселі з вузлом S або T, визначається ймовірністю того, що піксель знаходиться на передньому плані або на задньому плані. Вага між сусідніми пікселями визначається подібністю пікселів. Алгоритм для поділу графа знаходить мінімальний розріз зваженого графа. Нарешті, пікселі, підключені до вузла S, стають переднім планом, а пікселі, підключені до вузла T, стають фоном.

Висновок

Головною перевагою представленого алгоритму є його стійкість. Він розроблений з метою обробки зображень з різних пристроїв для отримання даних МРТ і з різною інтенсивністю. Це стає можливим за допомогою адаптивного порогового визначення та морфологічної реконструкції відтінків сірого, які отримують параметри за результатами статистичного методу суміші Гауса. За ним слідує алгоритм розрізання графа. Адаптивне порогове визначення та морфологічна реконструкція у відтінках сірого мають вирішальне значення для правильних результатів. Алгоритм розрізання графа підвищує точність сегментації в деяких конкретних випадках, але в цілому результати використання методу сегментації розрізання графа є менш вдалими порівняно з методом, який було виконано без розрізання графа.

к.т.н. Королько С.В. (НАСВ)

СИСТЕМА ВЗАЄМОДІЇ АРТИЛЕРІЙСЬКИХ ПІДРОЗДІЛІВ З ВИКОРИСТАННЯМ ОПТИЧНОГО ЛАЗЕРНОГО ЗВ'ЯЗКУ

Ефективна система управління артилерійськими підрозділами впроцесі виконання бойових завдань полягає в безперервній взаємодії управлінського та виконавчого органів.Ця взаємодія між окремими складовими в сучасних умовах може бути забезпечена лише з використанням сучасних надійних та безперебійних технологій зв'язку.

Традиційні системи підтримання зв'язку, які використовуються у військах, не в повній мірі відповідають сучасним вимогам та потребують переоснащення. Так, вивчення досвіду застосування технічних засобів у ході Українсько-російської війнисвідчить про виникнення проблемних питань щодо створення надійного і захищеного зв'язку, якийможна було б застосувати для систем дистанційного керування між структурними ланками управління та зразками озброєння.Широкого застосування в системах зв'язку набулодистанційне керування з допомогою радіозв'язку, яке застосовується в системах віддаленого управління різними об'єктами. Однак, такий зв'язок має ряд недоліків, оскільки може бути приглушений системами радіоелектронної боротьби, а використання дротового зв'язку під час інтенсивних дій ворога стає ускладненим. У зв'язку з цим пропонується проста і надійна система оптичного лазерного зв'язку.

До основних переваг лазерного зв'язку між керуючими і виконавчими об'єктами відносять відсутність заглушення чи виявлення оптичного лазерного зв'язку, можливість передавання великої кількості інформаційних даних, висока стійкість та стабілізація в умовах електромагнітного випромінювання та високий ступінь захисту ідешифрування.

Аналіз оптичної передачі інформаційних даних із застосуванням лазерного випромінювача тавідповідних відбивачів дозволив підвищити точність між приймально-передавальними об'єктами до декількох сантиметрів на віддалях від 0,5 до 3 км.При цьому отримано результати в напрямку формування надійного джерела сигналів випромінюваного та приймального пристроїв.Необхідна якість та дальність зв'язку буде залежати виключно від потужності лазерного випромінювання та пропускної здатності повітряного середовища. Найбільше для реалізації принципу надійності оптичного сигналу в якості джерела випромінювання підходять оптичні системи на базі напівпровідникових РЖБ сенсорів. Під час вибору діапазону оптичного зв'язку лазерного променя необхідно використовувати сигнали з більш високими частотами, наприклад УФ випромінювання, які будуть невидимі для ворога. Так, високоефективними оптичними системами вважаються сенсори на базі сенсорів «Canon». При цьому модулятор сигналів буде працювати в невидимій області 350-400 нм. Найпростіша лінія оптичного атмосферного зв'язку між двома пунктами буде складатися з приймального та передавального пристроїв, які розташовані у межах прямої видимості. У передавачі міститься лазер-генератор і модулятор його оптичного випромінювання. Модульований монохроматичний лазерний промінь спрямовується в сторону приймача. У приймачі відповідне випромінювання фокусується на фотоприймач в якому виконується його детектування і виділення інформації. Передавальна частина оптичної системи містить підсилювач сигналів, генератор струму і джерело випромінювання. Запропоновано використовувати атмосферний оптичний зв'язок в комплексі з системою БпЛА., яка б об'єднувала в собі взаємодію між випрямлячем та декількома передавачами сигналів. Це дасть можливість застосувати оптичні лазерні системи для використання на більші віддалі. Закордонний досвід взаємодії управлінської та виконавчої ланок показує, що система управління між складовими артилерійських підрозділів із застосуванням оптичного лазерного зв'язку буде розвиватись шляхом створення єдиного інформаційного середовища, що забезпечить обмін інформацією між органами й пунктами управління всіх ланок.

Косар О.Л. (ТОВ "ЮЕЙ ДЕФЕНС")
к.т.н. Гуржій П.М. (ВІТІ імені Героїв Крут)

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ЗАБЕЗПЕЧЕННЯ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ ТА ІНФОРМАЦІЙНОЇ ПІДРИМКИ "ICoMWare"

Вступ. Фахівцями ТОВ "ЮЕЙ ДЕФЕНС" розроблено програмно-апаратний комплекс "ICoMWare" (далі – ПАК), що призначений для інформаційної підтримки прийняття рішень командирами бойових розрахунків (підрозділів, екіпажів), забезпечення їх ситуаційної обізнаності та підвищення ефективності взаємодії підрозділів в умовах бойової обстановки шляхом створення єдиного інформаційного простору на мережецентричній основі.

Метою дослідження є підвищення ефективності управління підрозділами Сухопутних військ.

Виклад основного матеріалу дослідження

ПАК, в залежності від варіанту виконання, може встановлюватись як на броньовану і автомобільну техніку, так і експлуатуватися в будь-яких інших об'єктах, а його портативна версія забезпечить ситуаційну обізнаність диверсійно-розвідувальній або снайперській групі, корегувальнику артилерійського вогню, окремому солдату тощо.

Перевагами ПАК "ICoMWare" є:

• унікальне поєднання управлінської, комунікаційної, інтеграційної та безпекової складових;

• простота в експлуатації;

• використання програмного забезпечення власної розробки;

• автоматична побудова мережі передачі даних з використанням радіо- (КХ/УКХ), супутникових, радіорелейних засобів зв'язку, їх масштабування, одночасна інтеграція різнорідних мереж (Mesh, MANET);

• підтримка ієрархічних мереж (до 5 рівнів ієрархії) від рівня окремого військовослужбовця (екіпажу бойової машини) до рівня батальйону;

• робота по низькошвидкісних каналах зв'язку;

• контроль каналів зв'язку: сигналізація про втрату зв'язку, відсутність сигналу GPS, контроль якості обраного каналу зв'язку;

• захищений поштовий сервіс з підтримкою стандартного поштового клієнта;

• використання спеціального протоколу для гарантованої доставки повідомлень;

• підтримка попередніх версій програмного забезпечення;

• адаптація відображення інформації під екран будь-якого розміру;

• можливість постачання у різних комплектаціях відповідно до потреб споживача;

• можливість розширення функціоналу за рахунок розробки (інтеграції) інших програмних додатків відповідно до потреб споживач;

• реалізація інформаційного обміну з іншими системами та програмними комплексами, зокрема АС 9С701 ("Дзвін-АС"), ПК "Кропива", ПК "Термінал", БПАК "Фурія";

• використання персонального електронного ключа "Алмаз-1К", за допомогою якого забезпечується автентифікація користувача та шифрування даних для передачі між ПАК.

ПАК "ICoMWare" наказом Міністерства оборони України допущений до експлуатації у Збройних Силах України, має номенклатурний номер НАТО, код предмета постачання за ВК 001-2000 та рівень гарантій безпеки Г-2.

Висновки

За попередніми оцінками автоматизація процесів управління тактичного рівня на полі бою за допомогою використання ПАК "ICoMWare" може підвищити бойові можливості підрозділів до 15-20% і одночасно до 50% скоротити час, який витрачають органи управління на планування і доведення завдань до підлеглих.

Широке застосування ПАК "ICoMWare" створить підґрунтя для реалізації в ЗС України концепції ведення бойових дій в єдиному інформаційному просторі.

к.т.н. Крайнов В.О. (НУОУ ім. І.Черняховського)
Терновий О.В. (НУОУ ім. І.Черняховського)

ПРИНЦИПИ КОМПЛЕКСНОГО ПІДХОДУ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В умовах загрози інформаційній безпеці держави особливого значення набуває пошук нових можливостей забезпечення безпеки органів управління військового призначення з урахуванням формування нового поля протиборства – кіберпростору. На сьогоднішній день кіберпростір, через певну новизну, все ще не повністю нормативно врегульований на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення „акту війни" і можуть бути віднесені до операцій „відмінних від війни". Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світового співтовариства.

Активність з боку провідних держав світу у кіберпросторі, глибинні зміни ставлення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах у кіберпросторі, все це зумовлює застосування принципів комплексного підходу до забезпечення інформаційної безпеки вже на етапі проектування, впровадження та підтримки. Найбільш перспективною основою для побудови систем інформаційної безпеки є раціональне поєднання різних організаційних та програмно-технічних заходів та засобів з урахуванням вимог чинних нормативно-правових та нормативно-технічних документів.

При використанні автоматизованих інформаційних систем (АІС) в органах військового управління проблема забезпечення інформаційної безпеки все більш зростає. Цьому є цілий ряд об'єктивних причин.

1. Перш за все - це розширення сфери застосування засобів обчислювальної техніки і збільшений рівень довіри до автоматизованих систем управління і обробки інформації. Комп'ютерним системам довіряють найвідповідальнішу роботу, від якості виконання якої залежить ефективність роботи органів управління.

2. Змінився підхід і до самого поняття „інформація". АІС управляють технологічними процесами обробки та передачі секретної і конфіденційної інформації.

3. Проблема забезпечення інформаційної безпеки АІС стає ще більш серйозною і у зв'язку з розвитком і розповсюдженням обчислювальних сітей, територіально розподілених систем і систем з видаленим доступом до ресурсів, що спільно використовуються.

4. Доступність засобів обчислювальної техніки і, перш за все, персональних ЕОМ привела до розповсюдження комп'ютерних технологій, що закономірно, привело до збільшення числа спроб неправомірного втручання в роботу автоматизованих систем управління військами як із злим наміром, так і чисто „із спортивного інтересу". На жаль, багато хто з цих спроб має успіх і наносить значну утрату роботі органів управління.

5. Ще одним вагомим аргументом на користь посилення уваги до питань безпеки АІС є бурхливий розвиток і розповсюдження так званих комп'ютерних вірусів, здатних скрито існувати в системі і скоювати потенційно будь-які несанкціоновані дії.

6. Особливу небезпеку для АІС, комп'ютерних систем представляють зловмисники, фахівці - професіонали в області обчислювальної технікиі програмування, досконально знаючі всі достоїнства і слабі місця комп'ютерних систем і маючи в розпорядженні найдокладнішу документацію і найдосконаліші інструментальні і технологічні засоби для аналізу і злому механізмів захисту.

Кінцевою метою створення системи інформаційної безпеки є захист всіх категорій суб'єктів, прямо або побічно, що беруть участь в процесах інформаційної взаємодії, від

нанесення ним відчутного матеріального, морального або іншого збитку в результаті випадкових або навмисних дій на інформацію і системи її обробки і передачі.

В основі реалізації комплексного підходу до забезпечення інформаційної безпеки сьогодні лежать ще два принципи:

перший принцип полягає в тому, що абсолютно надійний, «непробивний» захист створити практично неможливо, оскільки необхідно розумне співвідношення витрат на захист інформації та можливих фінансових втрат від порушення інформаційної безпеки. Звичайно, перше безпосередньо залежить від фінансових можливостей органу управління.

Важливо також і ті, які витрати має зазнати зловмисник, щоб «розкрити» систему, і як вони співвідносяться з цінністю та актуальністю інформації, що зберігається в ній. Правильно збудовані системи повинні вимагати від золійника таких витрат часу або грошей на «розтин», щоб ця операція була безглуздою з практичної точки зору.

другий принцип передбачає, що система повинна бути гнучкою і легко адаптуватися до зовнішніх умов, що змінюються. Оскільки загрози інформаційній безпеці постійно стають дедалі витонченішими, у системі має бути закладено певний запас міцності як у частині програмно-технічних засобів, так і частині організаційних заходів безпеки. Комплексний підхід при створенні систем інформаційної безпеки передбачає, поряд із застосуванням технічних засобів захисту, вирішення питань упорядкування та управління ІБ на базі єдиної інтегрованої архітектури системи інформаційної безпеки, що реалізує такі принципи:

відповідність існуючим положенням щодо інформаційної безпеки;

інтегрування всіх необхідних підсистем, комплексів та технічних засобів;

універсальність, гнучкість та масштабованість архітектури, її повна керованість;

можливість варіювати склад та наповнення комплексів та підсистем;

забезпечення мінімальної сукупної вартості всього захисту.

Загалом комплексний підхід передбачає захист усієї інформаційної інфраструктури органів управління військового призначення від будь-яких несанкціонованих дій, тому дуже важливо, як із методичної точки зору буде організовано розробку такої системи. На цю годину склалася цілком певна послідовність розробки комплексних систем забезпечення інформаційної безпеки, яка включає кілька розглянутих нижче етапів. Найважливіші етапи в галузі комплексної інформаційної безпеки:

проектування, впровадження та супровід систем інформаційної безпеки, що забезпечують безпеку функціонування інформаційних ресурсів органів управління військового призначення;

комплексне діагностичне обстеження, оцінка та аудит систем інформаційної безпеки, у тому числі на відповідність існуючим стандартам.

Насамперед це вимагає активного реформування органів управління військового призначення; збільшення чисельності підрозділів, зайнятих у системі кіберзахіисту; розробки кіберозброєння та проведення пробних військово- розвідувальних акцій у кіберпросторі; посилення контролю за державнім інформаційним простором (способами доступу, контентом тощо). Необхідно посилити контроль з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі, що свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав та обов'язків громадянина та держави.

Таким чином, незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти мілітаризації кіберпростору, можна констатувати збільшення ролі суто військових структур у забезпечення інформаційної безпеки національної критично-важливої інфраструктури (національного кіберпростору). В таких умовах Україна має бути готова не лише до ведення оборонних війн, але активно створювати власні наступальні засоби ведення війни у кіберпросторі.

Куцаєв В.В. (ВІТІ ім. Героїв Крут)
Лазута Р.Р. (ВІТІ ім. Героїв Крут)
Куцаєв П.В. (ВІТІ ім. Героїв Крут)

ВАРІАНТ СХЕМИ ІНФОРМАЦІЙНОГО МОДЕЛЮВАННЯ

Людський мозок –
це найвища форма матерії,
яка відома людству.
В.В.

Вступ. Мозок людини або особистості (далі – ЛО) наслідує, формує, зберігає, корегує та постійно використовує індивідуальну модель світу людини – М*о*.

Модель світу М*о* має частку, яка унаслідується – $М_{old}$, та частку, яка формується й удосконалюється під час життєвого циклу ЛО – $М_{new}$ (1) [1].

$$Мо = М_{old} + М_{new}. \quad (1)$$

Модель світу людини М*о* постійно коректується ЛО у часі (2) [1].

$$Мо \rightarrow Мо(t) = М_{old}(t) + М_{new}(t). \quad (2)$$

Модель світу людини М*о*(*t*) складається з множини підмоделей μ_i, які стосуються всіх питань життя людини, в тому числі і наукових.

З початку людина унаслідує базову множину підмоделей $\mu_b(t_0)$, де їх кількість на момент часу (t_0) дорівнює *b* (3) [2].

$$Мо(t_0) \rightarrow \{\mu_1(t_0), \mu_2(t_0), \ldots, \mu_b(t_0)\}, \quad (3)$$

де *b* – кількість осмислених понять або підмоделей людини на початку її життя на час t_0;

$\mu(t_0)$ – первинна підмодель деякого терміна, знання, компетентності або досвіду людини щодо деякого питання, яка зафіксована в нейронах головного мозку людини у лексичній аудіоформі або відеомультиплікаційній формі зі смисловим навантаженням.

Зазначимо, що кількість підмоделей $\mu_1(t)$ у ЛО постійно зростає. Таке зростання будемо трактувати як накопичення життєвої та наукової інформації в комплексних нейронних згустках, які автори пропонують вважати матеріальними носіями біонейромоделей – $\mu_i(t)$, що зберігають знання та навички людини – $Мо_{new}(t)$ (4) [3].

$$Мо_{new}(t) \rightarrow \{\mu_1(t), \mu_2(t), \ldots\ldots\ldots, \mu_b(t), \ldots\ldots\ldots, \mu_{newt}(t)\}, \quad (4)$$

де $new_i(t)$ – кількість осмислених μ-підмоделей, придбаних людиною на час *t*.

Автори тези роблять наступне припущення: ЛО моделює всі необхідні їй життєві ситуації в особистому мозку. Таке моделювання допомагає їй жити та виживати. У науковця існує такий же процес моделювання.

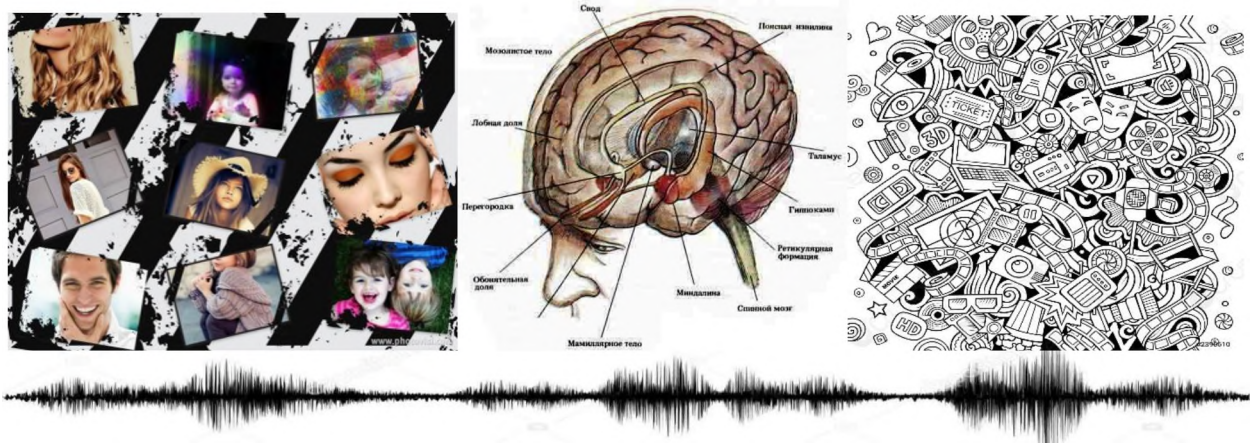


Рис. 1–4. Уявлення авторами центру моделювання мізансцен

Рисунки 1–4 пояснюють, що за кожним висловлюванням, терміном або думкою ЛО стоїть нейровузол, який пов'язує між собою аудіо- та відеофрагменти інформації з відповідних частинок головного мозку людини з часом їх запам'ятовування. Такий підхід дозволить в подальшому сформувати схему технічної обробки інформації на основі моделювання мізансцен.

Мізансцена – розташування акторів на сцені в певному поєднанні з навколишнім речовим середовищем (декорації, реквізит тощо) в ті чи інші моменти спектаклю [6].

Автори вважають, що мозок ЛО має можливість складати нові підмоделі $\mu_{newi}(t)$, які утворюють мізансцени щодо всіх різноманітних сцен, об'єктів, сценаріїв та процесів, які необхідні людині для її життя або для наукової діяльності. ЛО має можливість розмістити у своєму центрі уваги аудіолексичне речення, терміни, поняття, назви, які описують та складають мізансцену деякого процесу, явища або об'єкта [4]. При цьому головний центр моделювання ЛО складає пов'язану з підмоделлю $\mu_{newi}(t)$ складану мультиплікаційну аудіовізуальну мізансцену.

Надалі ЛО має можливість використовувати кожну підмодель $\mu_1(t)$ для програвання цього сценарію з різними вхідними даними – z, тим самим моделюючи різні варіанти розвитку подій, прогнозуючи хід подій та вибираючи раціональну поведінку.

Науковець таким же чином формує нову модель наукового питання $\mu\varkappa_{newi}(t)$ та одночасно вирішує наступні завдання:

розглядає модель $\mu\varkappa_1(t)$ з різними вхідними умовами z – $\mu\varkappa_1(t, z)$;

коректує саму модель $\mu\varkappa_1(t, z)$ до $\mu\varkappa_{new+1}(t, z)$, також різними умовами z;

перебирає z_i – вхідну інформацію, яка надходить до науковця.

На рис. 5 зображена спрощена схема створення наукової підмоделі $\mu\varkappa_{new1}(t,z)$ для обробки наукової інформації z.

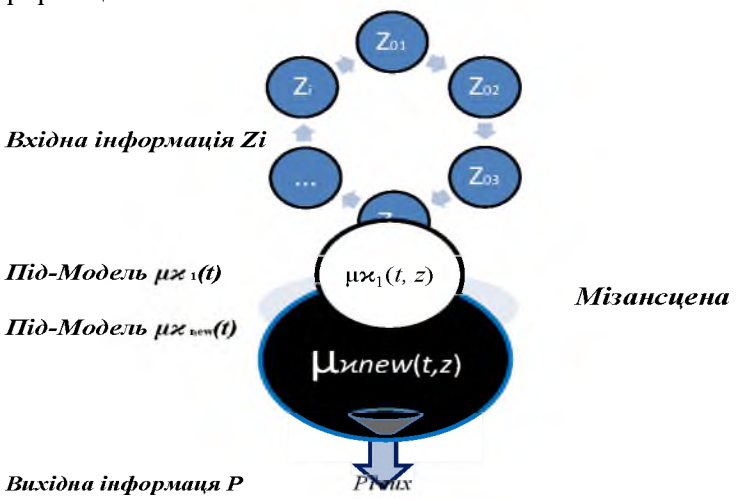


Рис. 5. Спрощена схема створення наукової підмоделі $\mu\varkappa_{new1}(t,z)$

Кожна підмодель $\mu_i(t)$ складає мізансцену, яка постійно використовується та модифікується в $\mu_{new}(t)$. Надалі укріплюється в мозку як достовірна на 100 %.

Науковець оперує набором підмоделей, понять і термінів $\{\mu_1(t_0), \mu_2(t_0), \ldots \mu_b(t_0)\}$, які зберігаються в біонейронному сховищі людини [4]. Кожна підмодель $\mu_i(t_0)$ постійно проходить апробацію та постійно покращується як все більш об'єктивна. Вектор, який пояснює логіку розвитку підмоделі $\mu_i(t_i,z)$ науковця з точки зору поступового досягнення оптимальності при вхідних даних z, виглядає наступним чином (5):

$$\begin{gathered} \text{підмодель } \mu_1(t_0, z) - 90\ \%; \\ \text{підмодель } \mu_2(t_1, z) - 95\ \%; \\ \ldots \\ \text{підмодель } \mu_i(t_i, z) - 99\ \%; \\ \text{підмодель } \mu_{i+1}(t_{i+1}, z) - 100\ \%. \end{gathered} \quad (5)$$

Науковець, маючи набір вхідних даних z_n та напрацьовані раніше наукові уявлення у вигляді підмоделей $\mu_i(t, z_1)$, проводить моделювання наукових мізансцен наступним чином:

спочатку вибирає підмодель $\mu_1(t, z)$;

розглядає результат – наукову мізансцену $p_1 = f(t, \mu_1(t_0, z))$;

обирає наступну підмодель $\mu_i(t, z)$;

розглядає результат – наукову мізансцену $p_i = f(t_i, \mu_i(t_i, z))$;

змінює підмодель $\mu_i(t, z)$ до $\mu_{newi+1}(t, z)$ та аналізує мізансцену $p_{newi+1} = f(t, \mu_{newi+1}(t_i, z))$.

Переробка старих моделей $\mu_{1\text{-}b}(t)$ до нових $\mu_{b+1}(t)$ створює вектор моделей $\{\mu_1(t_0), \mu_2(t_0), \ldots \mu_b(t_0), \ldots \mu_{newi}(t)\}$. На вершині такого процесу утворюються нові знання в підмоделі – $\mu_{newi}(t)$, які закріплюються у новому нейронному утворенні – вершині колонці згустків нейронів головного мозку людини, які чекають наступного циклу моделювання.

Рис. 6 пояснює місце збереження нових знань – нових підмоделей як згустків груп нейронів на вершині інформаційної колонки нейронів, які залежно від часу пов'язані з фіксованими у відповідних конфігураціях нейронів відео, аудіо та інших видів інформації.

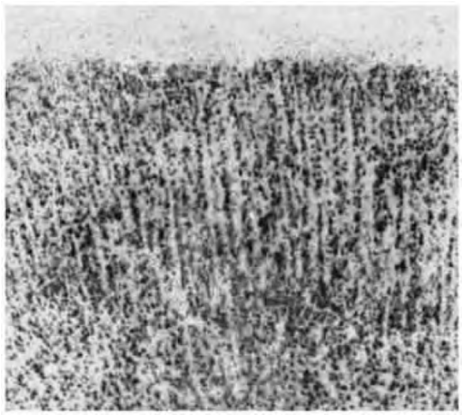


Рис. 6. Зображено колонки згустків ГН, які утворюються в головному мозку, тим самим створюючи пам'ять людини

Людський мозок вченого-науковця має величезну мотивацію щодо для творчої роботи. Це особливості людського мозку. Науковець підбирає відомі наукові базові підмоделі $\mu\varkappa_b(t_0)$ та загружає їх вхідними аудіо- та відеоданими – z_i, після чого намагається оцінити адекватність – a_b результатів моделювання p_b підмоделі $\mu\varkappa_b(t)$. У випадку, коли адекватність результатів недостатня, науковець поступово формує нову наукову підмодель $\mu\varkappa_{new}(t_{i+1}, z_i)$ та знову оперує вхідними даними z_i.

Висновки. Запропонована схема обробки наукової інформації передбачає моделювання мізансцен на основі використання базових наукових підмоделей $\mu\varkappa_b(t_i, z_i)$ з набором вхідних даних z_i. В наступному науковець поступово формує нову наукову підмодель $\mu\varkappa_{new}(t_{i+1}, z_i)$ та знову оперує вхідними даними z_i. Результатом є можливість створення нових машинних

підходів до обробки інформації, яка буде зафіксована у біонейроподібних сховищах та збережених у різний період часу.

У подальшому автори планують ряд спостережень за логікою та психологією науковців для осмислення схеми роботи нейронних згустків при моделюванні мізансцен під час пошуку наукової істини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цікаві факти про людський мозок. Частина II // Lytvynenko Clinic: центр неврології та реабілітації. URL: https://lc-neuro.com.ua/blog/czikavi-fakti-pro-lyudskij-mozok-chastina-ii (дата звернення: 19.10.2022).

2. Нова модель сприйняття: наш мозок бачить дуже багатий світ // Конкурент: інформаційне агентство. URL: https://konkurent.ua/publication/54312/nova-model-spriynyattya-nash-mozok-bachit-duzhe-bagatiy-svit/ (дата звернення: 19.10.2022).

3. Психологія навчання та психологічні проблеми навчання // Освіта.ua: тематичний ресурс. URL: https://osvita.ua/school/method/psychology/1665/ (дата звернення: 19.10.2022).

4. Ф. Блум, А. Лейзерсон, Л. Хофстедтер. Мозок, разум і поведінка. Редакція біологічної літератури. Переклад з англ. канд. біол. наук Є. З. Годіної // RoyalLib: електронна бібліотека. URL: https://royallib.com/book/blum_floyd/mozg_razum_i_povedenie.html (дата звернення: 19.10.2022).

5. К. Анохін. Мозок вченого: як він пізнає істину // YouTube: відеохостинг. URL: https://www.youtube.com/watch?v=npmuwIgO2Og (дата звернення: 19.10.2022).

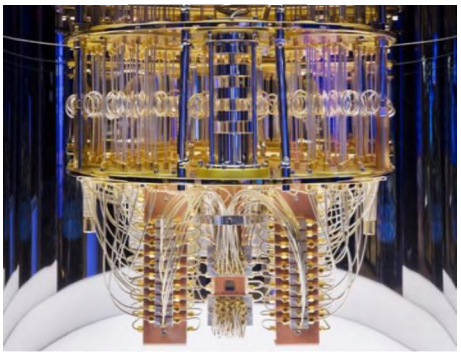
6. Мізансцена // Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki (дата звернення: 24.10.2022).

Куцаєв В.В. (ВІТІ ім. Героїв Крут)
Лазута Р.Г. (ВІТІ ім. Героїв Крут)
к.т.н.Орда М.В. (ЦВСД)
Дем'яненко Г.В. (НДЦ ЗС)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ

Метою тез є ознайомлення науковців з надпотужними можливостями квантових технологій, надання основ квантових обчислень та квантового зв'язку.

Актуальність. *Квантові розрахунки.* Сучасна теорія стверджує, що застосування квантових технологій (далі – КТ) призведе до стрибка у швидкості розрахунків для спеціальних завдань від 100 000 000 до 10 000 000 000 разів [1]. До таких спеціальних завдань можуть належати наступні:



створення квантового зв'язку, Інтернету та телепортації [2; 6; 10];
злам існуючих крипто шрифтів квантовим алгоритмом Шора [6;10];
проведення досліджень з ДНК [3];
розробки універсального штучного інтелекту [4];
створення нових складних матеріалів [4];
реалізація проєктів клінічних досліджень [5];
моделювання кліматичних умов [6];
моделювання складних систем [7];
створення каталізатора для абсорбування вуглекислого газу з атмосфери [8];
надпровідники, які здатні працювати при кімнатній температурі;
створення нових ліків від хвороб [9] та багато інших досліджень.

Останні 15 років у світі відбувається стрімкий розвиток засобів реалізації КТ. В основу КТ покладено заміна послідовного перемикання носія біту зі стану «0» на «1» за час $\Delta t_{біт} > 0$ на квантовий кубіт, побудований на основі квантових часток, де стани «0» та «1» існують одночасно на різних енергетичних рівнях квантової частки. Час перемикання «0» на «1» прагне до *0*, $\Delta t_{кубіта} \rightarrow 0$. Зі зростанням кількості *зв'язаних* кубітів потужність розрахунків зростає в геометричній прогресії [6; 10].

Кубіти та їх зв'язаність дозволяють квантовим комп'ютерам (далі – КК) досягнути *квантової переваги* над сучасними комплексами орієнтовно на 50-кубітовому КК.

Автори вважають, що слід інтенсивно готуватися до дій в пост квантовий період. КТ інтенсивно досліджують США, Канада, Великобританія, Германія, Франція, Китай, Австралія, Японія та рф) [1–9]. Розробки КТ успішно ведуть приватні компанії IBM, Intel, Швейцарська Quantique, Google, Microsoft, Amazon, Alibaba, Rigetti, IonQ, Toshiba канадська D-Wav, американська ВПК Northropp Grumman та ін.

Квантова перевага – означає момент, коли КК будуть вміти робити речі, на які не здатні звичайні комп'ютери. Концепція квантової переваги передбачає наявність унікальних особливостей КК, таких як квантова *заплутаність і суперпозиція.*

В табл. 1 вказані темпи росту зв'язаності кубітів і досягнення квантової переваги [1–12].

Таблиця 1

Держава / Компанія	Рік презентації КК	Кількість кубітів
США	2014 рік	5 кубіт
Intel	2017 рік	17 кубіт
Microsoft	2019 рік	50 кубіт
Досягнення стану квантової переваги над звичайним комп'ютером > 50 кубіт		
США / рф	2020 рік	51 кубіт
UMD / NIST	2017–2021 роки	53 кубіт
Rigetti Computing	2021 рік	80 кубіт (2 блоки*40 біт)
IBM	2021 рік	127 кубіт
IBM	2022-2025 рік	400–1 000 кубіт
КК компанії D-Wave One	2011 рік	з 128-кубітовим процесором.
D-Wave One	2025 рік	Планується створення 1024-кубітовим процес.
перспектива	2030 рік	1 000 000 кубіт

Квантовий зв'язок (далі – КЗ) — мережа зв'язку, де передача інформації здійснюється у вигляді кубітів між фізично розділеними квантовими процесорами [6; 10].

Квантове розподілення ключа – метод заснований на фундаментальних законах квантової фізики, коли процес виміру квантової системи змінює її стан. Зловмисник, який спробує вкрасти ключ, має якимось чином виміряти його, але вимір вводить аномалії, які бачать і легітимні учасники протоколу.

Квантова телепортація може стати наступним кроком у КЗ. Якщо у QKD криптографічні ключі поширюються із застосуванням КТ, при квантовій телепортації сама інформація передається із застосуванням зчеплених квантових пар.

Квантовий Інтернет – кінцева мета КЗ це створення мережі зчеплених між собою КК, підключених до ультразахищеного КЗ,

Кубіт – квантовий біт. Звичайний класичний біт може мати одне з двох значень: 0 або 1. Кубіт може мати значення, яке є або одним із них, або будь-яке інше значення, яке знаходиться між 0 та 1. Дане явище називається квантовою *суперпозицією* та, відповідно, може відбуватись лише в квантах – дуже маленьких об'єктах. Кубітом може виступати будь-який об'єкт, який має квантову поведінку, наприклад фотон.

Суперпозиція станів – кубіт, що знаходиться в суперпозиції, при вимірюванні колапсує в одне з двох детермінованих станів (0 або 1). Імовірність стану 1 або 0 визначається суперпозицією кубіта. Якщо кубіт знаходиться в рівній суперпозиції, то він знаходиться наполовину в стані 0, наполовину в стані 1.

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \quad (1)$$

Суперпозицію станів кубіта зображують графічно у вигляді координатної сітки на сфері, де кожний вузол відповідає певному стану, як зображено на рис. 1.

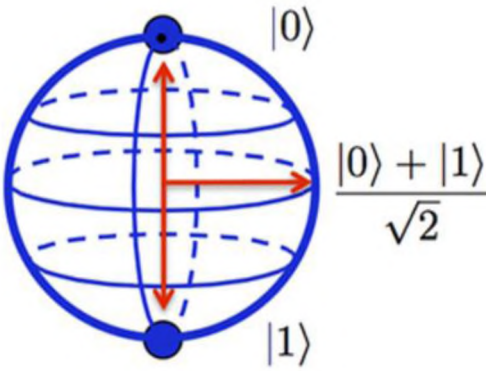


Рис. 1. Представлення кубіта

Стани $|0\rangle$ та $|1\rangle$ називають спеціальними станами обчислювального базису, які утворюють ортонормований базис цього векторного простору. Можливо виміряти біт, щоб визначити стан, в якому він знаходиться [10; 12].

Сфера Блоха. Сфера Блоха існує для графічного представлення кубітів. Стан кубіта (1) можна переписати у наступному вигляді:

$$|\psi\rangle=\cos\theta/2|0\rangle+e^{i\varphi}\sin\theta/2|1\rangle \quad (2)$$

Числа θ та φ задають точку на одиничній тривимірній сфері, як зображено на рис. 2. Сфера, зображена на рисунку, називається сферою Блоха. Вона існує для наочного представлення стану одиничного кубіта [10; 12].

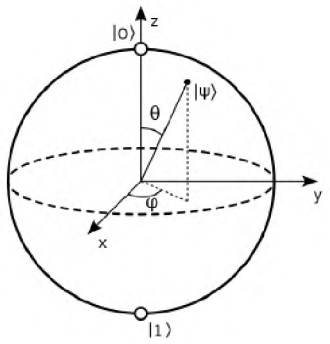


Рис. 2. Представлення стану кубіта на сфері Блоха

Вимірювання кубіта. Вимірювання відповідає неформальній ідеї «дивитись» на кубіт, який негайно **згортає квантовий стан** до одного з двох класичних станів 0/1 та 1/0.

Квантові обчислення. Фундаментальна модель квантових обчислень – квантові схеми. Квантовий комп'ютер будується з квантових схем, що складаються з дротів та елементарних квантових елементів, які дозволяють передавати квантову інформацію та маніпулювати нею [12]. Квантова схема є квантовою обчислювальною моделлю, побудованою з квантових логічних *ґейтів*, в яких обчислювальні кроки синхронізовано по часу. Входи квантових ґейтів зв'язані з входами схеми або виходами інших ґейтів. Складна унітарна операція може бути представлена у вигляді схеми, яка складається з кількох квантових ґейтів.

Вентилі Паулі. Вентилі Паулі – це одні з найпростіших квантових вентилів. Вентилі діють на один кубіт за раз.

Вентиль Паулі-X. Вентиль Паулі-X відповідає класичному вентилю NOT. Саме з цих міркувань вентиль-X також часто називається квантовим NOT-вентилем. На рис. 3 наведено приклад графічного зображення вентиля NOT.

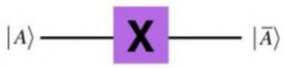


Рис. 3. Графічне зображення вентиля Паулі-X

Вентиль Паулі – Z. Елемент Z займає важливе місце в квантових схемах, він залишає стан $|0\rangle$ без змін, а $|1\rangle$ переводить в стан $-|1\rangle$.

Вентиль Паулі – Y. Елемент Y є комбінацією елементів X та Z. Даний елемент здійснює наступні перетворення: $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$

*Елемент Адамара***.** Елемент Адамара є фундаментальним квантовим вентилем. Елемент дозволяє нам відійти від полюсів сфери Блоха і створити *суперпозицію*. Елемент Адамара являє собою перетворення, які описуються наступною матрицею:

$$H=1/\sqrt{2}* \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}. \quad (3)$$

Елемент Адамара Відіграє ключову роль в багатьох квантових схемах, здійснюючи наступні перетворення:

$|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$

$|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$

На рис. 4 зображено однокубітні квантові елементи.

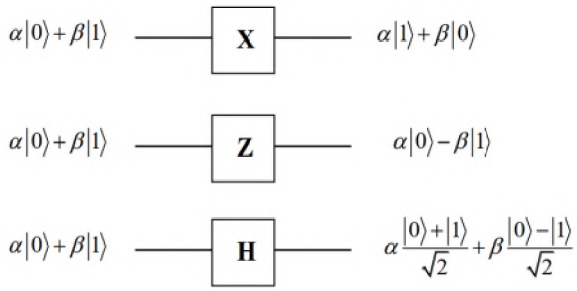


Рис. 4. Однокубітні квантові елементи та їх дія на квантовий стан

Фотон як кубіт. Різні фізичні сутності можуть бути використані як кубіти, включаючи іони, надпровідні заряди, спін атомного ядра тощо. Фотони мають деякі властивості, які роблять їх надзвичайно привабливими для використання в КК та для створення квантових каналів зв'язку.

Двоканальні кубіти (dual-rail qubits). Фотони рухаються по прямій. Отже, якщо обрано два шляхи руху і покладено фотон на будь-який з них, залежно від того, на якому шляху виявлений фотон, ми можемо сказати стосовно квантового стану фотону $|0\rangle$ або $|1\rangle$ відповідно. Двоканальний фотонний кубіт зображено на рис. 5.

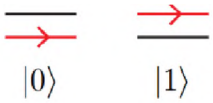


Рис. 5. Двоканальний фотонний кубіт. В залежності від того в якому каналі знаходиться фотон, стан кубіту є $|0\rangle$ або $|1\rangle$

Виявлення фотону. Життя фотона в квантовому експерименті починається з його генерації і закінчується його виявленням. Обидва процеси повинні бути ефективними, а їх продуктивність та властивості відіграють важливу роль у фотонних квантових обчисленнях.

Генерування фотонів. Детерміновані високоякісні джерела фотонів розробляються з використанням різноманітних фізичних систем, таких як захоплені іони та атоми, кольорові центри в діамантах, напівпровідники, квантові точки та інші, більш екзотичні методи.

Керування фотоном. Існує точний та детальний контроль поляризації фотона, траєкторією або статичним значенням часу завжди був силою ФКО.

Квантові помилки. Реальні системи страждають від небажаної взаємодії з зовнішнім світом. Ці небажані взаємодії виявляються як шум в квантовій системі обробки інформації. Потрібно розуміти та контролювати такі шумові процеси та квантові помилки при побудові квантових систем обробки інформації.

Квантові алгоритми. Будь-яку класичну схему можна замінити еквівалентною схемою, що містить оборотні (реверсивні) елементи, використовуючи реверсивні ворота Тоффолі. Ворота Тоффолі мають три вхідні біти та три вихідні біти, як показано на рис. 9 [6; 10].

Входи			Виходи		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

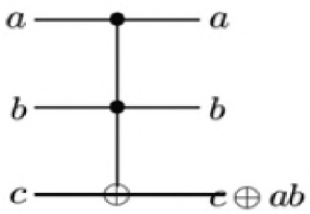


Рис. 9. Таблиця істинності для елемента Тоффолі та його схемна реалізація

Перевага квантових обчислень полягає в тому, що можуть бути обчисленими набагато потужніші функції за допомогою кубітів і квантових воріт.

Квантовий паралелізм. Квантовий паралелізм є фундаментальною особливістю багатьох квантових алгоритмів. Квантовий паралелізм дозволяє квантовим комп'ютерам оцінити функцію *f (x)* для багатьох різних значень *x* одночасно, як зображено на рис. 12.

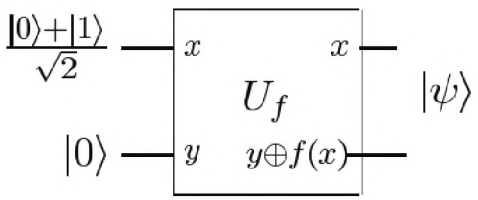


Рис. 12. Квантова схема для розрахунку f(0), f(1) одночасно. Uf квантова схема, яка трансформує входи, такі як $|x,y\rangle$ до $|x,y\oplus f(x)\rangle$

Пошук в базі даних. Прикладом ефективного квантового алгоритму є алгоритм пошуку інформації в невпорядкованій базі даних, іноді ще названий алгоритмом перебору. Алгоритм вирішення: даний неупорядкований набір з N предметів, знайти номер предмету, який співпадає з даним зразком. Класичний метод послідовного порівняння зразку зі всіма предметами потребує в середньому $N/2$ порівнянь. Запропонований Гровером квантовомеханічний алгоритм потребує порядку $\sqrt{N}$ кроків [6; 10]. Практична користь даного методу велика. Будь-яку таку задачу можна вирішувати повним перебором методу Гровера – перевірку правильності рішення можна вставити в алгоритм порівняння S.

Розробка програм та запуск на квантовому комп'ютері. Продемонструємо принцип дії елементу Адамара, логічного вентиля Паулі X та операції порівняння. В ході програми задіяно два кубіти: до одного задіяний елемент Адамара, а до іншого – вентиль Паулі X, який спрацьовує при істинному значенні (квантовий стан $|1\rangle$) першого кубіта, який завдяки дії елементу Адамара знаходиться в суперпозиції. Таким чином утворюється квантова заплутаність, коли квантовий стан одного кубіта впливає на стан іншого [10].

Програма може бути запущена на класичному комп'ютері, використовуючи спеціальне програмне забезпечення, яке імітує КК. Також відбувся запуск програми на справжньому КК компанії IBM. Для запуску програми потрібно зайняти чергу [10].

Програмне забезпечення. В якості програмного забезпечення можливо використати Qiskit програмне забезпечення з відкритим кодом для роботи з КК на рівні схем, імпульсів та алгоритмів [10]. Основна мета Qiskit – створити стек програмного забезпечення, який дає змогу користування КК кожному, незалежно від рівня їх кваліфікації. Qiskit дозволяє легко розробляти експерименти й програми та запускати їх на реальних КК або класичних тренажерах. Qiskit підтримує Python 3.6 або новіші версії. Використовуємо Qiskit версії 0.26.2. Офіційний сайт: https://qiskit.org [10].

Аналіз отриманих результатів. Отримані результати підтверджують, що нинішній КК IBM, який використовує електрони, як кубіти має певні погрішності, що пов'язані з квантовими помилками та декогерентністю. Комп'ютер, який буде розроблений на фотонній системі, матиме меншу погрішність та стане більш доступним у використанні. Переваги, які має фотон, дають йому дуже велику перспективу бути використаним як кубіт в КК [10].

Висновки:

1. Логічно припустити, що розвиток КТ призведе до вагомих наслідків, а саме:

буде створено КК з величезною обчислювальною перевагою над звичайними ПК;

наразі у світі здійснюється практична реалізації фрагментів КЗ, квантової телепортації та квантового (захищеного) Інтернету;

створення КТ загрожує сучасним стандартам шифрування даних.

2. Революційний розвиток КТ може призвести до ситуації типу «Енігма», коли Британія зламала «надійну» систему шифрування зв'язку німецького командування та таємно використовувала цю інформацію

3. Використання КТ призведе до надзвичайної інформаційної переваги того, хто першим ними оволодіє, тому підрозділам ВЗ та КБ доцільно будувати відповідні засоби, алгоритми та сценарії дій з урахуванням тактики постквантового періоду [11].

4. Наразі відомі компанії починають надавати в аренду робочий час на квантових системах. Це відкриває шляхи для застосування КТ у різноманітних наукових дослідженнях.

В подальшому автори планують приступити до вивчення інструментарію, необхідного для створенні квантових алгоритмів та їх практичного використання на КК. В майбутньому можливо проведення складних розрахунків в інтересах військових досліджень із застосуванням КТ, орендуючи час КК в компаніях IBM, Intel, Google та ін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Китай створив квантові комп'ютери у 10 млн. разів потужніше суперкомп'ютера // URL: https://https://focus.ua/digital/496363-v-kitae-sozdali-kvantovye-kompyutery-v-10-mln-raz-moshchnee-lyubogo-superkompyuter (дата звернення: 16.09.2022).

2. Це справжня телепортація. Вченим вперше вдалося передати інформацію квантовою мережею // URL: https://techno.nv.ua/ukr/innovations/kvantoviy-internet-50246228.html (дата звернення: 10.09.2022).

3. Квантові комп'ютери // URL: https://phm.cuspu.edu.ua/nauka/naukovo-populiarni-publikatsii/1026-kvantovi-kompyutery-mriya-chy-realnist (дата звернення: 14.09.2022).

4. Квантовий комп'ютер – нова ера на порозі // URL: https://nrfu.org.ua/news/kvantovyj-kompyuter-nova-era-na-porozi (дата звернення: 15.09.2022).

5. Квантово-фармакологічні дослідження властивостей антиоксидантів як лікарських засобів // URL: https://www.umj.com.ua/article/75175/kvantovo-farmakologichni-doslidzhennya-vlastivostej-antioksidantiv-yak-likarskix-zasobiv (дата звернення: 15.09.2022).

6. Остапов С. Е., Добровольський Ю. Г. Квантова інформатика та квантові обчислення: навч. посіб. Чернівці: ЧНУ, 2021. 99 с.

7. Квантово-фармакологічні дослідження властивостей антиоксидантів як лікарських засобів // URL: https://comsys.kpi.ua/upload/Комп'ютерне моделювання (дата звернення: 10.09.2022).

8. Комп'ютерне моделювання//URL:https://www.umj.com.ua/article/75175/kvantovo-farmakologichni-doslidzhennya-vlastivostej-antioksidantiv-yak-likarskix (дата звернення: 15.09.2022).

8. П'ять технологічних трендів, які врятують людство / URL: https://techno.nv.ua/ukr/technoblogs/novi-tehnologiji-50127580.html (дата звернення: 15.09.2022).

9. Квантові комп'ютери: що це, як працюють, які перспективи // URL: https://blog.allo.ua/ua/kvantovi-komp-yuteri-shho-tse-yak-pratsyuyut-yaki-perspektivi_2018-07-39/ (дата звернення: 15.09.2022).

10. Філоненко Є. О. Фотонні системи з однокубітними квантовими обчисленнями. Київ: Кафедра мікроелектроніки НТУ України «КПІ імені Ігоря Сікорського» Факультет електроніки, 2021.

11. Горбенко І. Д., Качко О. Г., Кузнєцов О. О., Потій О. В., Горбенко Ю. І., Пономар В. А., Єсіна М. В. Проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення // Доповідь на конференції BITI, 2018р. URL: https://iit.com.ua /

12. Карлаш Г. Ю. Квантові інформаційні системи: навч. посіб. для спеціальності «Прикладна фізика та наноматеріали». Київ: факультет радіофізики, електроніки та комп'ютерних систем Київського національного університету імені Тараса Шевченка, 2018. 77 с.

Легкобит В.С. (ВІТІ ім. Героїв Крут)
Анохін Д.Л. (ВІТІ ім. Героїв Крут)
Бурда Є.А. (ВІТІ ім. Героїв Крут)
Власенко О.В. (ВІТІ ім. Героїв Крут)

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ НАВЧАЛЬНО-ПЕДАГОГІЧНОЮ ТА НАУКОВО-ТЕХНОЧНОЮ ДІЯЛЬНІСТЮ ВВНЗ

У країні продовжуються процеси діджиталізації інститутів суспільства, важливу роль відіграє цифровізація процесів навчально-педагогічної та науково-технічної діяльності військового вищого навчального закладу (ВВНЗ). Інформаційні технології, які впроваджені в діяльність ВВНЗ є потужним інструментом підвищення ефективності навчання та наукових досліджень, служать істотним фактором, що забезпечує якість освіти. Сучасні вищі навчальні заклади являють собою складні технічні та організаційні системи, які вимагають оперативної реакції на процеси, що відбуваються в них. Тому виникає необхідність у створенні інформаційної системи для здійснення та підтримки навчальної, наукової та управлінської діяльності ВВНЗ на основі сучасних інформаційних технологій.

Метою дослідження є проведення детального аналізу процесів діяльності ВВНЗ, керівних документів, які регламентують дані процеси, а також аналіз існуючих інформаційних систем з визначенням їх основних переваг і недоліків. Створення інформаційної системи для управління навчально-педагогічною та науково-технічною діяльністю вищого військового навчального закладу. Для досягнення вказаної мети у роботі сформульовано наступні часткові завдання:

1. Аналіз керівних документів та процесів діяльності ВВНЗ.
2. Постановка завдань досліджень та створення архітектури інформаційної системи управління навчально-педагогічною та науково-технічною діяльності ВВНЗ.
3. Аналіз існуючих технології та засобів для реалізації поставлених завдань.
4. Розробка проекту технічного завдання на створення інформаційної системи управління навчально-педагогічною та науково-технічною діяльності ВВНЗ.
5. Розробка інформаційної системи управління навчально-педагогічною та науково-технічною діяльності ВВНЗ.

За результатами аналізу існуючих інформаційних систем встановлено, що більшість програмних рішень являються вузько направленими, дозволяють вирішити обмежений спектр завдань, не охоплюють всі процеси діяльності ВНЗ, особливо управління. Процеси управління навчально-педагогічною та науково-технічною діяльністю у ВВНЗ , на відмінну від інших фахових ВНЗ мають певні специфічні відмінності. Тому актуальним є створення спеціалізованої інформаційної системи саме для ВВНЗ. Архітектура системи буде складатись з двох основних підсистем: підсистема керування навчально-педагогічною діяльністю та підсистема керування науково-технічною діяльністю, які будуть мати загальну інформаційну базу і інтерфейси для взаємодії. Інформаційна система буде спрямована на вирішення наступних основних завдань: зарахування та відрахування курсантів (слухачів); контроль академічної успішності; формування робочих навчальних планів; розподіл навчального навантаження між факультетами, кафедрами та викладачами; формування штатного розкладу; складання та коригування розкладів занять та іспитів; облік навчальних матеріалів та наукових праць; ведення електронного документообігу тощо.

Наявність інформаційної системи управління навчально-педагогічною та науково-технічною діяльністю ВВНЗ дозволяє не тільки уніфікувати роботу з інформацією, прискорити процеси її обробки, швидко вирішувати завдання оперативного управління та отримувати однаково достовірні відповіді на питання, що виникають з різних напрямків діяльності інституту, а й приймати вірні управлінські рішення.

Висновки. Отже, в рамках даної роботи було проаналізовано керівні документи, які регламентують процес діяльності ВВНЗ, було визначено функціонал системи та розроблену проект технічного завдання та архітектуру інформаційної керування навчально-педагогічною та науково-технічною діяльністю ВВНЗ.

д.т.н. Лисенко О.І. (КПІ ім. Ігоря Сікорського)
к.т.н. Явіся В.С. (КПІ ім. Ігоря Сікорського)
Гетьман О.В. (КПІ ім. Ігоря Сікорського)

МЕТОД БАГАТОКРІТЕРІАЛЬНОГО ВИБОРУ МОВНИХ КОДЕКІВ З УРАХУВАННЯМ НАБОРУ ПОКАЗНИКІВ ЯКОСТИ

Якість передачі мови істотно залежить як від типу та способу побудови мережі, так і від алгоритму кодування мовної інформації – кодека. Тому, ще на етапі проектування мережі необхідно визначитись – який мовний кодек буде застосований.

Всі існуючі типи мовних кодеків за принципом дії можна розділити на три групи [1]:

- Кодеки з імпульсно-кодовою модуляцією (ІКМ, Pulse Code Modulation – PCM) і адаптивною диференціальною імпульсно-кодовою модуляцією (АДІКМ, Adaptive differential pulse-code modulation – ADPCM).
- Кодеки з вокодерним перетворенням мовного сигналу.
- Комбіновані (гібридні) кодеки.

Показники якості мовних кодеків взаємозалежні й суперечливі. Часто кодеки описують п'ятьма показниками якості: k_1 – швидкість кодування, k_2 – оцінка якості кодування мови, k_3 – складність реалізації, k_4 – сумарна затримка, k_5 – розмір кадру [2].

Швидкість кодування визначає вимоги до пропускної здатності каналу.

Оцінка якості кодування мови з використанням різних кодеків здійснюється за допомогою характеристики MOS (Mean Opinion Score), це усереднена сукупна думка по 5-бальній шкалі.

Складність алгоритму кодування пов'язана з необхідними обчисленнями в реальному часі. Складність алгоритму визначає швидкість обробки, вимірювану в мільйонах операцій у секунду (Million Instructions Per Second, MIPS). Складність обробки впливає на фізичні розміри кодуючого, декодуючого або комбінованого пристрою, а також на його вартість і споживану потужність.

Часова затримка збільшується зі збільшенням розміру кадру, а також зі збільшенням складності алгоритму кодування. При передачі мови припустима затримка в одному напрямку не може бути більше 250 мс.

Оскільки розмір кадру з однієї сторони впливає на якість відтвореної мови, а з іншого боку – на затримку переданої інформації, пов'язану з обробкою, то такий показник можна виключити, врахувавши його значення шляхом корегування k_2, k_4.

Більшість кодеків описані рекомендаціями сімейства «G» стандарту H.323. Їх основні характеристики наведені в таблиці 1.

Таблиця 1. Основні характеристики кодеків.

Кодек	**Метод компресії**	**Швидкість кодування (k_1)**	**Якість, MOS (k_2)**	**Складність реалізації (k_3)**	**Затримка (k_4)**
G.711	PCM	64 Кбіт/с	Висока 4,1	Низька (8 MIPS)	Дуже низька (0,75 мс)
G.726	ADPCM	32/24/16 Кбіт/с	Середня 3,96 (32 Кбіт/с),	Низька (8 MIPS)	Дуже низька (1 мс)
G.729	CS-ACELP	8 Кбіт/с	Середня 3,92	Висока (30 MIPS)	Низька (10 мс)
G.729A	CA-ACELP	8 Кбіт/с	Середня 3,7	Помірна (20 MIPS)	Низька (10 мс)
G.723.1	MP-MLQ ACELP	6,4/5,3 Кбіт/с	Середня 3,87 (6,4 Кбіт/с),	Помірна (16 MIPS)	Висока (37 мс)
G.728	LD-CELP	16 Кбіт/с	Середня 3,61	Дуже висока (40 MIPS)	Дуже низька (3-5 мс)

Вибір алгоритму кодування мови залежить від вимог до якості, характеристик каналу, що є у розпорядженні, можливостей реалізації певного алгоритму з погляду на складність обчислень.

Відомий спосіб вибору варіанта мовного кодека методом аналізу ієрархій складається в декомпозиції проблеми вибору єдиного варіанта системи на прості складові частини й одержанні чисельних даних суджень експертів по парних порівняннях різних елементів проблеми вибору. У результаті обробки отриманих даних виходять оцінки компонентів вектору глобальних пріоритетів, що характеризує пріоритетність порівнюваних варіантів системи. Але цей спосіб вимагає складних обчислень, тому пропонується інший підхід.

Сам процес вибору буде складатися із двох етапів. На першому виконується приведення показників до однотипного характеру і їх нормування, на другому – безпосередньо обчислення абсолютних значень оцінок кожного кодека. Результати заносяться в таблицю 2.

У нижньому рядку таблиці 2 зазначені вагові коефіцієнти (значимість) p_i відповідного показника, які визначаються досвідченими експертами на основі даних про проектовану мережу.

Абсолютна оцінка S для кожного кодека обчислюється відповідно до виразу:

$$S = \sum_{i=1}^{4} k_{i\text{н}} \times p_i,$$

де $k_{i\text{н}}$ – перетворені нормовані показники якості кодека;

p_i – вагові коефіцієнти відповідних показників якості кодека.

Пріоритет віддається кодеку, що має найбільше значення абсолютної оцінки.

Таблиця 2. Приклад результатів обчислень абсолютних оцінок кодеків.

Кодек	**Показники якості**				**Абсолютна оцінка кодека**
	Швидкість кодування ($k_{1\text{н}}$)	**Якість, MOS ($k_{2\text{н}}$)**	**Складність реалізації ($k_{3\text{н}}$)**	**Затримка ($k_{4\text{н}}$)**	
G.711	0,10	1,00	1,00	1,00	0,58
G.726	0,20	0,97	1,00	0,75	0,59
G.729	0,80	0,96	0,27	0,08	0,71
G.729A	0,80	0,90	0,40	0,08	0,71
G.723.1	1,00	0,94	0,50	0,02	0,83
G.728	0,40	0,88	0,20	0,19	0,50
Вагові коефіцієнти	0,47	0,30	0,15	0,08	

Запропонований алгоритм вибору мовного кодека потребує незначної кількості обчислювальних процедур та забезпечує урахування основних показників якості з ваговими коефіцієнтами, що дозволяє експертам надавати пріоритет певним показникам залежно від характеристик мережі та її основного призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вакуленко О.В., Явіся В.С. Методика вибору мовних кодеків термінальних пристроїв інфокомунікаційних мереж // VIII Науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО». Збірник тез. – К.: ВІТІ. – 2015. – С. 228-229.

2. Явіся В.С. Методика вибору мовних кодеків // Десята міжнародна науково-технічна конференція «Проблеми телекомунікацій». Матеріали конференції. – К.: НТУУ «КПІ». – 2016. – С. 501-503.

к.т.н. Ліщинська Х.І. (НАСВ)
к.ф.-м.н. Сеник А.П. (НУЛП)
Іваник І.Ю. (НУЛП)
Сеник Ю. А. (НЛТУ)

ВІЗУАЛІЗАЦІЇ ТА ПРОГНОЗУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Актуальність. Сьогодні, в епоху значних інформаційних потоків, аналіз даних з метою їх відокремлення та сортування потребує все більше зусиль. Візуальні інформаційні системи прискорюють та спрощують цей процес а також дозволяють швидко виділити найважливіше. Відомо, що більшість людей сприймають візуальні дані краще, ніж текст, адже згідно з дослідженнями 90% інформації, що надходить у мозок людини, – це зображення, тому він обробляє їх значно швидше. Під візуалізацією даних мається на увазі подання інформації у графічній формі, наприклад, у вигляді кругової діаграми, графіка або візуального подання іншого типу. Якісна візуалізація інформаційного потоку має критичне значення для аналізу та прогнозування даних, а також прийняття рішень на цій основі. Візуалізація дозволяє продуктивно помічати та інтерпретувати зв'язки і взаємини, а також виявляти тенденції, що розвиваються, які не привернули б уваги у вигляді несистематизованих даних. Найчастіше для інтерпретації графічних уявлень не потрібно спеціальне навчання, що скорочує можливість підготовки користувачів.

Більшість засобів візуалізації даних можуть підключатися до локальних або хмарних джерел даних, наприклад, реляційних баз. Таким чином, дані вилучаються для аналізу, а користувачі можуть вибрати найбільш відповідний спосіб їх представлення з кількох варіантів. В мережі Інтернет широко присутні спеціалізовані програмні продукти для візуалізації даних та аналітики, що використовуються для аналізу великих обсягів даних. Найпопулярнішими у застосуванні є наступні: Tableau (www.tableau.com), BI Domo (www.domo.com), Looker (https://looker.com), Qlik Sense (www.qlik.com), Board (www.board.com). Перечислені програмні продукти застосовуються для управління активами і ризиками шляхом проведення поглибленого аналізу, формування звітів та моделювання проектної діяльності, що дозволяє розробляти довготермінові стратегії.

Метою роботи. Створення та опис функціональних можливостей інформаційної системи, яка із застосуванням вбудованих в CRM-систему Salesforce методів візуалізації та прогнозування дозволяє використати динамічну диверсифікацію при управлінні проектом і може використовуватись як консультативний інструмент.

Основні положення. Для отримання динамічних даних, з метою тестування інформаційної системи, застосовуються відкриті дані від Yahoo Finance (https://finance.yahoo.com). З метою обробки інформації в середовищі Salesforce із застосуванням інструментарію звітності та візуалізації Reports та Dashboards а також Tableau CRM (CRM Analytics) організовані звіти, що дозволяють фільтрувати дані, з використанням яких створюються інформаційні панелі їх візуалізації. Окрім зручної візуалізації у запропонований проект системи включено можливості визначення закономірностей за допомогою вбудованого в середовище Salesforce штучного інтелекту та статистичного аналізу а також інструмент Einstein Discovery for Reports. Даний інструмент демонструє кореляцію поля, для якого проводився аналіз, у порівнянні з іншими, долученими у звіт полями. Чим більше отримане відсоткове значення, тим вища статистична залежність даних один від одного. Також Einstein Discovery пропонує різні аналітичні висновки, які зміг статистично отримати штучний інтелект.

Висновки. Запропонований проект інформаційної системи може застосовуватись для аналізу та прогнозування можливих ризиків, а також для підтримки динамічної диверсифікації в процесі планування ефективних у вибраний часовий проміжок стратегічних рішень.

Лютов В.В. (ХНУПС)

ВИКОРИСТАННЯ МЕТОДУ ROOT-MIN-NORM У СТЕПЕНЕВОМУ БАЗИСІ ДЛЯ ВИДІЛЕННЯ РАДІОСИГНАЛУ ПРИ ВПЛИВІ ЗАВАД

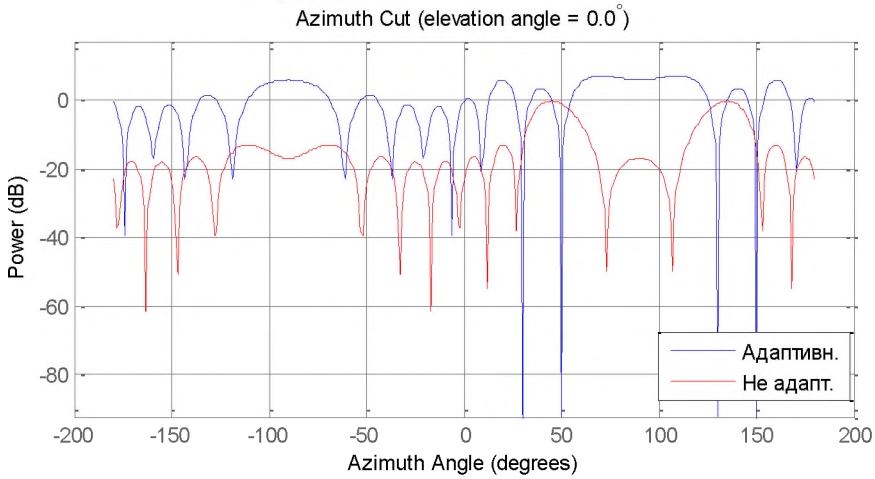
Досвід ведення російсько-української війни свідчить про широке використання засобів радіозв'язку, безпілотних та роботизованих засобів і комплексів, велику кількість радіолокаційних та інших радіовипромінюючих засобів, що працюють в умовах лавіноподібного зростання кількості радіовипромінюючих засобів в активній фазі ведення бойових дій та широкого застосування противником засобів радіоелектронної боротьби. Враховуючи це, виникає нагальна потреба зменшення впливу чисельних навмисних та випадкових завад на корисний сигнал та його виділення в умовах складної завадової обстановки. Одним з перспективних напрямків вирішення зазначеної задачі є розробка методів підвищення просторової та частотної селекції на основі використання методів спектрального оцінювання з надрозділенням, що дозволяють виділяти корисний сигнал на фоні завад та підвищувати відношення сигнал-шум (ВСШ) корисного сигналу. Часткове вирішення завдань підвищення ВСШ корисного сигналу у багатопроменевому каналі зв'язку виконано у стандарті IEEE 802.11ac, де реалізовано режим адаптивного формування діаграми спрямованості (beamforming) для MU-MIMO режиму, що дозволяє формувати до 4 незалежних потоків даних декільком користувачам формуючи в напрямку кожного з них окрему діаграму. Проте, цей стандарт не забезпечує селекцію близько розташованих (менше Релеевської межі) корисного та завадового сигналів в частотному або в просторовому спектрах, що є характерним для умов військової експлуатації при постановці завад корисному сигналу засобами РЕБ противника.

Вирішення задач селекції сигналів за частотою або в просторі здійснюється методами спектрального аналізу. Методи засновані на використанні швидкого перетворення Фур'є мають недостатню роздільну здатність (не перевищують Релеевської межі) та значно поступіються методам спектрального аналізу з надрозділенням здатним ефективно виділяти корисний сигнал при впливі на нього завадою або при кутовій чи частотній дисперсії корисного сигналу (швидке переміщення джерела радіосигналу) в умовах багатопроменевого каналу зв'язку. Проте, основним стримуючим фактором використання методів спектрального аналізу з надрозділенням для оцінки каналу зв'язку є їх значна обчислювальна складність. Для зменшення обчислювальної складності методу спектрального аналізу з надрозділенням ROOT-MIN-NORM в [1] запропоновано замість розкладення кореляційної матриці вхідної послідовності використовувати розкладення в степеневий ряд характеристичним поліномом, що на порядок з (O^3 до O^2) зменшує обчислювальну складність.

Отже, метою доповіді є представлення результатів моделювання процесу відновлення корисного сигналу методом спектрального аналізу з надрозділенням ROOT-MIN-NORM у ступеневому базисі, при впливі на нього завад, що перевищують корисний сигнал за рівнем потужності та мають однакові частотні та близькі просторові спектри.

Дослідження було проведено з використанням системи імітаційного моделювання Matlab. При моделюванні були використані системний об'єкт phased.IsotropicAntennaElement System ™ та програмні додатки Phased Array System Toolbox™ і Communications Toolbox ™ системи Matlab. В якості сигналу було використано 16-QAM модульований сигнал, одиничної амплітуди, з кутом надходження корисного сигналу 45 градусів по азимуту. Прийнятий сигнал містить тепловий шум, що має Гаусівський закон розповсюдження з нульовим математичним очікуванням, одиничною дисперсією і потужністю 0.5 Вт. Таким чином на кожному елементі ЛЕАР забезпечується ВСШ на рівні SNR=3 дБ, що за умов відсутності інших джерел випромінювання дозволяє забезпечити формування діаграми спрямованості (ДС) в напрямку джерела сигналу, забезпечуючи при цьому підвищення ВСШ до 8 разів і нормальну роботу приймача.

Для моделювання впливу засобу РЕБ противника, на приймальну антену ЛЕАР надходять завади з напрямків в 30 та 50 градусів по азімуту, та амплітудою, яка на порядок перевищує корисний сигнал (рис 1. переривчата лінія). За таких умов, навіть при підвищенні ВСШ до рівня *SNR=50 дБ*, звичайний (без адаптивної обробки) прийом сигналу не відбувається. Відновлення прийому відбувається лише при відстроюванні завадових сигналів на 30 градусів по азімуту від корисного сигналу (45±30 градусів). При цьому, в режимі без адаптивного формування ДС із загальної кількості переданих біт – 30714, отримані з помилками 9850 біт, що складає 32.07% від загальної кількості переданих біт, тобто імовірність бітових помилок складає $P_b = 3.2 \cdot 10^{-1}$ (рис.2).



Рисонок 1. – Адаптивний та неадаптивний методи формування ДС, в адаптивному методі в напрямку завад сформовані провали ДС, і максимум ДС в напрямку корисного сигналу.

Реалізуючи адаптивне формування ДС в напрямку на корисний сигнал, ми спочатку використовуючи метод спектрального аналізу ROOT-MIN-NORM у ступеневому базисі визначаємо кути надходження сигналів та завад. Після чого формуємо ДС MIMO системи в напрямку корисного сигналу, а провали діаграми спрямованості в напрямку завад (рис.1, суцільна лінія). Такий підхід, навіть за наявності завад, дозволяє підвищити ВСШ з *SNR=3 дБ*, до *SNR=41.88 дБ*. При цьому, імовірність бітових помилок складатиме $P_b = 1.6279 \cdot 10^{-4}$. Це означає, що з загальної кількості переданих 30714 біт повідомлення, помилки виявлені лише в 5 бітах, або 0.02% помилкових біт від загальної кількості.

Таким чином, використання оцінок кутів надходження сигналів джерел випромінювання обчислених запропонованим методом Root-Min-Norm у ступеневому базисі в задачах адаптивного формування ДС, дозволяє підвищити ВСШ з 2.84 дБ до 41.88 дБ і за рахунок адаптивного формування ДС, усунути негативний вплив завадових сигналів та підвищити достовірність отриманої інформації, яку представимо імовірністю правильного прийому переданих символів і, яка складає для неадаптивного режиму 0.68 та адаптивному 0.99 відповідно.

На підставі отриманих даних проведеного моделювання, можна зробити висновок про доцільність впровадження режимів адаптивного формування ДС, що використовують вимірювані значення просторового та частотного спектрів методами спектрального аналізу з надрозділенням в задачах просторовій селекції сигналів і значним чином може підвищити рівні розвід- та завадозахищеність каналу радіозв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лютов В.В. Алгоритм адаптивного управління параметрами MIMO системи шляхом вимірювання кутових координат сигналів методом Root-Min-Norm у степеневому базисі. / В.В. Лютов // Новітні технології – для захисту повітряного простору: 16 міжнар. наук. конф. Харк. нац. ун-ту Повітряних Сил імені Івана Кожедуба, 10–11 квітн. 2020 р. : тези допов. – Х., 2020. – С. 229.

Ляшенко Г.Т. (ВІТІ ім. Героїв Крут)
Шемендюк О.В. (ВІТІ ім. Героїв Крут)
Бохно Т.Р (ВІТІ ім. Героїв Крут)
Ткач В.О. (ВІТІ ім. Героїв Крут)

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ЗАБЕЗПЕЧЕННЯ СИТУАЦІЙНОЇ ОБІЗНАНОСТІ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ

Вступ (актуальність або постановка задачі)

Агресія російської федерації викрила низку проблем, пов'язаних підтримкою прийняття рішень під час управління підрозділами тактичної ланки під час планування та ведення бойових дій. Зокрема, в підрозділах тактичної ланки (особливо на рівнях екіпаж/відділення-взвод-рота-батальйон) відсутні автоматизовані системи, які забезпечують командирам підрозділів ситуаційну обізнаність з використанням сучасних радіостанцій КХ та УКХ діапазонів (Harris, Aselsan, Elbit). Наявні в Збройних Силах програмні продукти та системи є централізованими за своєю архітектурою, потребують високошвидкісних каналів та не забезпечують надійний захист інформації (не мають відповідних сертифікатів Державної служби спеціального зв'язку та захисту інформації України). Винятком є вітчизняний програмно-апаратний комплекс "ICoMWare".

Метою дослідженняє підвищення ефективності управління підрозділами тактичної ланки за рахунок підвищення ситуаційної обізнаності командирів підрозділів.

Виклад основного матеріалу дослідження

Програмно-апаратний комплекс "ICoMWare" (далі – ПАК) призначений для забезпечення ситуаційної обізнаності та інформаційної підтримки командира підрозділу (екіпажу бойової машини) та відповідних посадових осіб пунктів управління тактичної ланки при виконанні завдань за призначенням з метою підвищення ефективності управління шляхом створення єдиного інформаційного простору на мережецентричній основі.

Відповідно до застосування, ПАК розроблений у таких варіантах виконання:

- ПАК "ICoMWare" (бортовий варіант виконання) – для встановлення на броньовану техніку (танк, БТР, БМП, САУ тощо) та автомобільну техніку (КШМ, ШМ, КАЗ тощо);
- ПАК "ICoMWare" (стаціонарний варіант виконання) – для встановлення на пунктах управління (спостережних командних пунктах) підрозділів тактичного рівня (взвод, рота, батальйон);
- ПАК "ICoMWare" (портативний варіант виконання) носимою версією ПАК та призначений для забезпечення мобільних груп (розвідувальних, диверсійних, груп артилерійського наведення, груп евакуації поранених тощо) з метою збору та передачі органам управління інформації (розвідувальних даних, координат цілей, координат поранених, коригування вогню артилерії тощо);
- ПАК "ICoMWare" (на базі ноутбука у захищеному виконанні/планшета у захищеному виконанні, що призначений для: індивідуального застосування – окремим військовослужбовцем (в пішому порядку, при переміщенні на бойовій машині або розташуванні на пункті управління).

ПАК "ICoMWare" має ряд ключових особливостей, реалізованих в управлінській, телекомунікаційній, інтеграційній та безпековій складових.

В управлінській складовій ПАК реалізовано:

• набір сервісів, що забезпечують ситуаційну обізнаність (створення єдиної картини тактичної обстановки) в режимі "online";

• набір сервісів, що забезпечують підтримку та автоматичний перерахунок різних систем географічних координат (СК-42, УСК2000, WGS84, UTM, MGRS);

• набірсервісів, щозабезпечуютьобмінповідомленнями та ведення тактичного чату;

• набір сервісів, що забезпечують контроль показників бойової готовності до виконання завдання, отримання інформації щодо радіусів ураження основною і додатковою зброєю обраної бойової одиниці, отримання інформації щодо зон прямої видимості;

• вирішення ряду інформаційно-розрахункових задач тактичного рівня.

В телекомунікаційній складовій реалізовано:

• автоматична побудова завадостійкої тактичної mesh-мережі засобами ПАК;

• набір сервісів, що забезпечують автоматичне визначення типу та параметрів підключеної радіостанції, автоматичний збір даних про топологію радіомережі та автоматичну побудову мережі передачі даних з використанням цифрових радіостанцій зі швидкістю передачі даних від 9600 біт/с;

•протокол гарантованої доставки повідомлень, що актуально в умовах не стійкого радіозв'язку;

• набір сервісів, що забезпечують внутрішню та зовнішню комунікацію (циркулярний або адресний обмін інформацією;

• сервіс синхронізації тактичної обстановки;

• набір сервісів, що забезпечують голосовий зв'язок;

• набір сервісів, що забезпечують контроль стану каналів зв'язку.

Характерною рисою телекомунікаційної складової є те, що програмно-апаратні комплекси достатньо під'єднати до радіостанцій радіомережі і система автоматично побудує мережу передачі даних між відповідними абонентами без додаткових налаштувань програмно-апаратних комплексів чи радіостанцій.

В інтеграційній складовій реалізовано:

• API для інтеграції з іншими системами та програмними комплексами (на сьогодні реалізована інтеграція з АС 9С701 ("Дзвін-АС"), ПК "Кропива", ПК "Термінал", БПАК "Фурія");

• набір сервісів, що забезпечують підключення датчиків (сенсорів) та іншого обладнання (відеокамер, засобів GPS-навігації, систем внутрішнього зв'язку та комутації, систем датчиків бойової машини);

• набір сервісів, що забезпечують підключення засобів електронної розвідки (електронних біноклів, далекомірів, приладів нічного бачення, тепловізорів, БПЛА) через HDMI інтерфейс або додатковий інтеграційний модуль.

Архітектура системи побудована таким чином, що здатна забезпечити інтеграцію будь-яких цифрових джерел інформації, автоматизованих систем чи програмних комплексів на вимогу Замовника (Споживача) шляхом нескладного та швидкого додавання програмних інтеграційних модулів.

Безпековаскладова створена у відповідності до НД ТЗІ 2.5-008-2002:

• користувачі з різними правами (ролями);

• ідентифікація та автентифікація користувачів в системі;

• моніторинг дій користувачів;

• розподілінформації на тактичну та технологічну;

• криптографічнийзахистінформації.

Програмно-апаратний комплекс може працювати з використанням персонального електронного ключа"Алмаз-1К", за допомогою якого забезпечується автентифікація користувача та шифрування даних для передачі між ПАК за ДСТУ ГОСТ 28147:2009.

Крім того,ПАК "ICoMWare" має номенклатурний номер НАТО, код предмета постачання за ВК 001-2000 та рівень гарантій безпеки Г-2 за вимогами НД ТЗІ 2.5-004-99.

Висновки

Впровадження подібних систем в тактичній ланці управління підвищує ситуаційну обізнаність командирів підрозділів під час планування та ведення бойових дій, забезпечує інформаційну підтримку під час прийняття управлінських рішень, підвищує ефективність застосування бойових потенціалів підрозділів тактичної ланки, забезпечує високі показники стійкості, безперервності, оперативності та скритності управління.

Маркін А. В. (ТОВ «Асельсан Україна»)
Пономарчук К.М. (ТОВ «Асельсан Україна»)

СУЧАСНІ ТЕХНІЧНІ РІШЕННЯ ТА ТЕНДЕНЦІЇ РОЗВИТКУ В ГАЛУЗІ ВІЙСЬКОВОГО ЗВ'ЯЗКУ КОМПАНІЇ ASELSAN

Актуальність. Системи зв'язку стандарту LTE останнім часом набирають все більшу популярність у світі. Крім того вже існують певні зразки військової техніки, які виробляються з використанням стандартів зв'язку стандарту LTE. Зазначені системи набувають все більшої важливості у військову військовій справі. Застосування таких систем надасть можливість підвищити спроможність органів військового управління у користуванні системами зв'язку, інформаційними системами та сучасними сервісами зв'язку. Крім того можливість забезпечення взаємосумісності таких систем з іншими засобами зв'язку, такими як радіостанції програмно визначеної архітектури (SDR) може бути здійсненна за рахунок використання сучасної системи внутрішнього зв'язку ICS 6670, яка може застосовуватися як бойових машинах так і в органах військового управління.

Основна мета та задача доповіді. Донесення до учасників II Міжнародної науково-технічної конференції інформації про останні технічні рішення та тенденції розвитку в галузі військового зв'язку компанії Aselsan

Основні положення. Широкосмугові рішення компанії Aselsan з використанням стандартів зв'язку стандарту LTE втілені у вигляді Базової Станція Aselsan-Ulak Lte-A Macrocell, яка широко протестована в сільській/міській місцевості, на відкритому повітрі/у приміщеннях, у випадках масових заходів та у вигляді Гібридного Портативного Терміналу 3800, який поєднує в собі широкосмуговий (LTE) та вузькосмуговий (DMR+P25) діапазони. Ці рішення за допомогою IP мереж можуть бути з'єднані з мережами професіонального зв'язку силових структур та військовими мережами радіостанцій Aselsan програмно визначеної архітектури (SDR). Програмно визначені радіостанції це система радіозв'язку, у якій компоненти, які традиційно впроваджуються у застарілих радіостанціях (наприклад, змішувачі, фільтри, підсилювачі, модулятори/демодулятори, детектори.) замість апаратного мають програмне виконання, що дозволяє втілювати в одній радіостанції до п'яти режимів роботи, що дорівнює п'ятьом повноцінним аппаратним виконанням радіостанцій різних діапазонів та видів модуляції, способу передачі даних. В свою чергу, радіостанції Aselsan мають систему внутрішнього зв'язку на основі IP – ICS 6670, що застосовувється як на бойових машинах так і в органах військового управління і дозволяє забезпечити передачу даних та голосовий зв'язок за технологією VoIP з використанням методів шумозаглушення радіомережами Aselsan, Motorola, Harris.

Висновок: Керівництво та колектив ТОВ «Асельсан Україна» сподівається на те, що доповідь про останні технічні рішення та тенденції розвитку в галузі військового зв'язку компанії Aselsan надасть можливість учасникам конференції застосувати цю інформацію на користь державних інтересів України та Збройних Сил України, сприятиме подальшому плідному співробітництву між Турцією та Україною.

к.т.н. Марченко А.О. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

МАТЕМАТИЧНА МОДЕЛЬ АДАПТИВНОЇ ЗА ПОЛЯРИЗАЦІЄЮ АНТЕННОЇ РЕШІТКИ ДЛЯ РАДІОРЕЛЕЙНИХ СТАНЦІЙ

Анотація. Розглянуто математичну модель адаптивної за поляризацією антенної решітки на основі двошарової поляризаційно-голографічної антени шляхом удосконалення відомого методу інтегральних рівнянь першого роду.

Summary. A mathematical model of a polarization-adaptive antenna array based on a two-layer polarization-holographic antenna is considered by improving the well-known method of integral equations of the first kind

Ключові слова: математична модель, електромагнітна хвиля, поляризація, адаптивна антенна решітка, анізотропна структура, метод інтегральних рівнянь першого роду.

Антенні системи (АС) радіорелейних станцій (РРС) випромінюють (приймають) електромагнітні хвилі (ЕМХ) у напрямку передачі (прийому) інформації. Такі АС будуються на основі антен, які мають великий коефіцієнт підсилення та вузьку діаграму спрямованості (ДС), але, як правило, мають лінійну поляризацію. Під час радіорелейного зв'язку ЕМХ поширюються уздовж земної поверхні, при цьому напрямок вектору електричної складової ЕМХ може змінюватись, тому якість приймання сигналів погіршується за рахунок послаблення їх потужності.

Крім того, для збільшення пропускної здатності цифрових РРС використовуються технологія Multiple Input Multiple Output (множинний вхід – множинний вихід) (MIMO). Недоліком такої технології є те, що для забезпечення зв'язку в АС використовуються додаткові антени, що ускладнює конструкцію РРС.

Тобто під час організації зв'язку за допомогою РРС існує проблемна ситуація, яка обумовлена потребою забезпечити швидкісний та надійний зв'язок в умовах поширення ЕМХ уздовж земної поверхні без енергетичних втрат сигналів.

Для одночасної реалізації технології MIMO та усунення неузгодженості поляризації пропонується використання двошарових адаптивних за поляризацією антенних решіток (АР) на основі поляризаційно-голографічних антен (ПГА), які мають властивість перетворення сигналів з будь якою поляризацією в колову. Таким чином можна побудувати двошарову поляризаційно-голографічну антену (ДПГА), як набір анізотропних структур потрібної конфігурації (голограм). Діаграми спрямованості ДПГА формуються за рахунок поляризаційних ефектів голограм двох решіток у відповідних діапазонах частот. ПГА будуються вже розробленими методами конструктивного синтезу, але існуючи математичні моделі та методи конструктивного синтезу, що описують процес поширення ЕМХ потребують удосконалення для ДПГА.

Конструктивний синтез ДПГА проводиться за такою послідовністю: для заданих просторових ДС розраховується амплітудно-фазове розподілення (АФР) електромагнітного поля та визначаються конструктивні параметри АР, які реалізують потрібний АФР.

ДПГА розглядається як анізотропна (неоднорідна за діелектричною проникливістю) структура. Тому формалізація математичної моделі адаптивної АР зводиться до синтезу фазового розподілення на імпедансному тілі методом інтегральних рівнянь (ІР) першого роду, що ґрунтується на рішенні крайової задачі дифракції ЕМХ та дає змогу визначити голографічне ядро, яке фізично відповідає шару АР. Рішення ІР залежить від виду його ядра, яке з фізичного погляду описує імпедансні властивості тіла та має бути самоспряженим.

Формалізація математичної моделі адаптивної за поляризацією АР методом інтегральних рівнянь першого роду дає змогу описати дифракцію ЕМХ на двошаровому імпедансному тілі. Подальшим напрямом досліджень є розроблення математичного методу конструктивного синтезу для опису процес поширення ЕМХ в антенах такого типу для РРС.

к.т.н. Масесов М.О. (ВІТІ ім. Героїв Крут)
Новицький Д.В. (ВІТІ ім. Героїв Крут)
Шугалій О.О. (ВІТІ ім. Героїв Крут)
Пономаренко З.М. (ВІТІ ім. Героїв Крут)

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ MIMO У ЗАСОБАХ РАДІОЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

За результатами проведеного аналізу функціональних можливостей та технічних характеристик засобів радіозв'язку, що впроваджуються та використовуються останнім часом в провідних країнах світу, підтверджуються подальші тенденції застосування сучасних методів цифрової обробки сигналів та високоефективних методів модуляції.

Серед перспективних інформаційних технологій, впровадження яких дозволило здійснити перехід до засобів зв'язку наступного покоління, слід зазначити використання наступних технологій: цифрової обробки сигналів, багаторівнених видів модуляції сигналів, ортогональної (неортогональної) частотної дискретної модуляції (OFDM та N-OFDM), направлених і smart-антен (цифрових антенних решіток), антенну технологію множинного входу – множинного виходу (MIMO).

Окремої уваги заслуговує використання технології MIMO, яка активно впроваджується у засобах зв'язку, в тому числі військового призначення, останніми роками. Технологія просторового рознесення каналів передачі та прийому дозволяє кратно збільшити (в залежності від кількості антен, що використовуються) пропускну спроможність у радіоканалі та / або рівень сигнал/шум.

Серед світових лідерів виробництва засобів зв'язку з використанням технології MIMO з початку 2000-х років залишається компанія "Silvus Technologies" (США). В результаті високотехнологічної інтеграції та застосування сучасних технологій MIMO та MANET у поєднанні з багаторівневими сигнальними конструкціями забезпечується бездротова передача на високих швидкостях мультисервісного трафіку (відео, аудіо та даних) на полі бою. Радіостанції забезпечують: роботу в широкому частотному діапазоні (400 МГц – 6 ГГц); високу завадозахищеність (власна формі хвилі та особливості модуляції); низьку затримку пакетів (<10 мс / канал (hop)); збільшення дальності радіозв'язку; високий рівень захищеності інформації, яка циркулює в мережі (шифрування AES 256/ FIPS 140-2); гнучкість формування та організації (зміни конфігурації) радіомережі на полі бою. Крім того, слід зазначити, що сучасні радіостанції серії StreamCaster типу SC4400E та SC4200E реалізовані у захищеному виконанні зі ступенем захисту IP68.

Функціональні та технічні характеристики зазначених радіостанції дозволяю визначити наступні основні сфери їх застосування:

забезпечення високошвидкісного доступу до телекомунікаційних ресурсів на пункті управління при розгортанні абонентської радіомережі;

забезпечення персонального радіозв'язку між військовослужбовцями з високою пропускною спроможністю для передачі будь-яких видів трафіку;

побудова складних та самоорганізуючих радіомереж на полі бою в складних умовах при постійній зміні конфігурації мережі у режимі самоорганізації;

використання в якості авіаційної радіоплатформи для збільшення дальності зв'язку (десятки кілометрів) та масштабованості забезпечення зв'язку.

Наведені характеристики та можливості станцій серії StreamCaster було підтверджено в ході практичних досліджень, що проводились в умовах, наближених до реальних умов експлуатації. Результати проведених досліджень дозволили визначити найбільш доцільні сфери та варіанти застосування станцій, а також сформувати пропозиції щодо комплектації та їх подальшого використання у Збройних Силах України.

Михайлюк С.С. (ВІТІ ім. Героїв Крут)
к.т.н. Борисов О.В. (ВІТІ ім. Героїв Крут)
к.т.н. Борисов І.В. (НДІ ВР)

ЖИВУЧІСТЬ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ ЗАГАЛЬНОГО ТА СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

На даний час обговорюється проблема, пов'язана з застосуванням робототехнічних комплексів в телекомунікаційних системах і мережах загального та спеціального призначення, які широко застосовуються в різних областях, особливо у надзвичайних ситуаціях. Телекомунікаційні системи і мережі загального та спеціального призначення являють собою апаратно-програмні технічні пристрої, які використовуються для підтримки прийняття управлінських рішень, забезпечують збільшення ефективності при прийнятті рішень, підвищення зручності користування та розширення функціональних можливостей. Однак, незважаючи на те, що робототехніка інтенсивно використовується для розширення людських можливостей в небезпечних і недоступних середовищах, тісного об'єднання телекомунікаційних систем і мереж загального та спеціального призначення та робототехнічних комплексів не існує.

Створення на основі робототехнічних комплексів складних єдиних платформ дозволяє використовувати ці платформи у низці нових областей: інформаційний та комунікаційний напрями; енергетика; фізичний розподіл (включаючи транспортування); життєво важливі служби (аварійно-рятувальна та урядові служби). Прикладні області критичних платформ сильно різняться. Однак існують загальні характеристики, які мають відношення до живучих систем.

Живучість визначається здатністю платформи продовжувати надавати послуги в умовах різних типів відмов і збоїв. Основним механізмом, за допомогою якого живучість може бути досягнута в критичних ситуаціях, є відмовостійкість.

Архітектури платформ, на яких критично важливі програми пристосовані до послуг галузей промисловості, неминуче перебувають під впливом витрат та вигідних компромісів. Крім того, є кілька інших подібних характеристик, якими володіють критично важливі платформи в багатьох сферах застосування та які мають відношення до вимоги живучості системи:

гетерогенні вузли. Незважаючи на велику кількість вузлів на багатьох з цих платформ, часто невелике число вузлів має більш важливе значення для функціональності платформи, ніж решта. Це відбувається через те, що критичні частини функціональності платформи реалізовані лише на одній або невеликій кількості вузлів. Неоднорідність поширюється також на апаратні платформи, операційні системи, прикладне програмне забезпечення і навіть авторитетні домени;

композитна функціональність. Послуга, що постачається кінцевому користувачу, часто реалізується за допомогою комп'ютера з різними функціональними можливостями на різних вузлах. Таким чином, зовсім різні програми, що запускаються на різних вузлах, надають різні послуги, а повний спектр послуг можна отримати тільки тоді, коли кілька підсистем співпрацюють та працюють у певній зумовленій послідовності. Це зовсім не схоже на звичні додатки, такі як сервери маршрутизації пошти через Інтернет;

стилізовані пункти зв'язку. У багатьох випадках критично важливих додатків інфраструктури використовуються виділені посилання точка-точка, а не пов'язані повністю між собою чистою роботою. Причини такого підходу з'являються через включення робіт додатків, які вимагають більш високий рівень безпеки, і вимоги повного підключення;

вимоги до робочих характеристик. Деякі критичні інформаційні системи, як система фінансової компенсації, мають м'які обмеження в режимі реального часу, вимоги до пропускної спроможності (наприклад, для перевірки розрахунку в секунду), в той час як інші, такі як частини багатьох систем транспортерів та управління енергією, мають жорсткі

обмеження в режимі реального часу. У деяких системах вимоги до експлуатаційних характеристик змінюються з часом в якості навантаження або функціональних змін. Наприклад, протягом періоду від кількох годин у фінансових системах або протягом певного періоду днів чи місяців у транспортних системах;

вимоги до безпеки. Виживання визначається шкідливими атаками, а також викликаними апаратними та програмними збоями. Враховуючи важливість критичної структури додатків, їх інформаційні системи залучають терористів, які мають намір зірвати і саботувати повсякденне життя. Навмисні помилки, шкідливі атаки становлять значний інтерес для стратегії аналізу несправностей;

значний обсяг бази даних. Додатки інфраструктури залежать, в першу чергу, від даних. Багато їх використовують кілька великих баз даних, розташованих на різних вузлах, і з більшістю баз даних пов'язано дуже велика кількість операцій;

застаріла матеріальна база. Через вартість і зручність критичні структури додатку часто використовують дешеві компоненти обладнання, операційних систем, мережевих протоколів, систем баз даних і додатків. Крім того, ці системи містять застарілі компоненти або виконане за індивідуальним замовленням програмне забезпечення, яке використовувалося системою протягом багатьох років.

Зазначені вище характеристики є важливими, більшість з них, ймовірно, залишаться такими у платформах майбутнього. Але темпи впровадження нових технологій в ці платформи та введення абсолютно нових типів компонент відбувається швидко, і вони припускають, що методи аналізу повинні враховувати можливі характеристики майбутніх систем. Можна припустити, що наступними будуть важливі архітектурні аспекти майбутніх платформ:

збільшення кількості вузлів. Кількість вузлів у мережах інфраструктури, швидше за все, різко зростатиме в міру покращення функціональності, продуктивності та доступу користувачів. Вплив всього цього на відмовостійкість є значним. Зокрема, виявлення помилок та відновлення повинні бути регіональними у тому сенсі, що для різних частин мережі знадобляться різні стратегії відновлення. Крім того, також передбачається, що зусилля щодо реалізації будуть збільшуватися, тому що, ймовірно, у багатьох регіонах буде багато різних очікуваних помилок, для кожної з яких потрібні різні способи виявлення;

зростаючий рівень резервування. Зі зниженням вартості обладнання буде зростати надмірність, яка вбудована в компоненти низькорівневих систем. Як приклад можна вказати дзеркальні диски та резервні групи серверів. Це спростить проблему відмовостійкості у разі несправності низького рівня. Тим не менш, нелокальні, катастрофічні помилки будуть вимагати виявлення та відновлення стратегії, аналізу, корелюючи інформацію про помилки, координуючі відновлення та зміну конфігурації декількох вузлів;

мережі із комутацією пакетів. За багатьма причинами Інтернет стає мережевою технологією вибору будівництва нових систем, незважаючи на низький рівень безпеки і відсутність гарантій виконання. Однак, перехід до мереж із комутацією пакетів, будь то Інтернет або віртуальні приватні мережі, здається неминучим, як і наслідки вирішення підходів для забезпечення відмовостійкості.

Слід зазначити необхідність вираховування та документування всіх подій та обставин, які можуть призвести до серйозної втрати або порушення служби платформи.

На практиці необхідно проводити аналіз небезпек для визначення вразливих місць платформи та загроз, які викликають занепокоєння. Імовірність різних подій потрібно визначити, а потім має бути проведено аналіз вимог.

До того ж, повна специфікація живучості повинна документально точно відповідати запропонованому рівню обслуговування системи для всіх можливих пошкоджень, для яких потрібна обробка та відновлення платформи.

Отже, необхідно мати чотири складові для забезпечення надійних платформ: усунення несправностей, відмовостійкість, прогнозування та попередження помилок.

к.т.н. Міхєєв Ю.І. (ЖВІ ім. С.П. Корольова)
Павленко М.М. (ЖВІ ім. С.П. Корольова)

ВИКОРИСТАННЯ МЕРЕЖЕВОГО СЕРВІСУ GOOGLE "КАРТИ"ДЛЯ ВЕДЕННЯ БАЗИ ДАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

Актуальність. Одночасно із широкомасштабним вторгненням російської федерації в Україну ворог також активізував свої сили в напрямі інформаційної боротьби. Наразі противник використовує всі можливі інформаційні ресурси для того щоб у якомога найкоротші терміни досягнути цілей своїх інформаційно-психологічних операцій. Такі умови вимагають раціонального розподілу завдань під час проведення ефективних заходів з протидії психологічним впливам противника.

Постановка задачі. Використання соціальних інтернет-сервісів в інтересах інформаційно-психологічних операцій набуває особливої актуальності. Наявні цифрові комунікації дозволяють користувачам мережі "Інтернет" безкоштовно отримувати інформацію та обмінюватися нею. Разом із отриманням різноманітного контенту користувачі мережі "Інтернет" стають вразливими до інформаційно-психологічного впливу, який є непомітним і його ознаки можна виявити лише згодом. Отже, в інформаційній війні переважає той, хто швидше наповнює необхідним контентом інформаційний простір, у якому перебуває визначена цільова аудиторія. Це завдання передбачає виконання певних етапів, серед яких основними є: розроблення спеціального контенту, вибір та підготовка каналів для його розповсюдження та безпосереднє розповсюдження контенту.

Основні положення. Під час вибору каналів для розповсюдження контенту у соціальних мережах слід проаналізувати можливість отримання інформації цільовою аудиторією в конкретному районі (регіоні, області). Далі на основі отриманих результатів необхідно сформувати перелік інформаційних джерел (груп у соціальних мережах) з яких цільова аудиторія у подальшому буде отримувати спеціально підготовлений контент. У процесі знаходження нових інформаційних джерел, які в подальшому використовуватимуться для розповсюдження контенту, виникають такі завдання:

ведення (корегування) списку нових інформаційних джерел (додавання, прибирання, внесення змін);

систематизація та структурування списку інформаційних джерел;

організація спільного доступу до списку інформаційних джерел між учасниками групи розповсюджувачів спеціального контенту;

подання списку інформаційних джерел у зручний спосіб.

Вирішення указаних завдань можна забезпечити шляхом використання існуючих сучасних програмних додатків, систем управління базами даних або додаткового існуючого чи розробленого спеціального програмного забезпечення. Для візуального подання інформаційних джерел пропонується використати цифрову карту.

У доповіді наведено приклад подання списку інформаційних джерел за допомогою загальнодоступного мережевого сервісу Google "Карти". Сервіс Google "Карти" має певний функціонал для нанесення маркерів на цифрову карту. Кожен з маркерів має набір властивостей, таких як: форма, колір, текстове та графічне поле, які заповнюються за необхідності та зберігаються у базі даних. У текстове поле можна заносити посилання на відповідні інформаційні джерела (групу соціальної мережі) та довідкову інформацію, наприклад, кількість підписників у групі соціальної мережі, а в графічне поле –відповідні логотипи. Дані про інформаційні джерела, розподілені за регіональною доступністю до них цільової аудиторії, можливо зберігати в окремих шарах карти. Це дозволяє швидко обирати інформаційні джерела для розповсюдження в них контенту на цільову аудиторію у визначеному районі.

Висновок. Таким чином, використання запропонованого підходу дозволить частково оптимізувати процес розповсюдження спеціального контенту в соціальних інтернет-сервісах.

Мішок А.А. (ДНДІ ВС ОВТ)
Тертишнік Є.М. (ДНДІ ВС ОВТ)
Ратушний С.В. (ДНДІ ВС ОВТ)
Потапов О.І. (ДНДІ ВС ОВТ)

КІБЕРЗАХИСТ ДЕРЖАВНИХ СТРУКТУР ТА ОРГАНІЗАЦІЙ В УМОВАХ ВІЙНИ

У сучасному світі кількість кібератак зростає з року в рік, що змушує задуматися про важливість того, щоб національні структури та організації були готові завчасно реагувати на кіберзагрози. Дослідження та впровадження новітніх заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури є актуальним питанням сьогодення.

Державна служба спеціального зв'язку та захисту інформації України підтвердила, що в період з лютого по березень 2022 року на українські організації було скоєно близько 2800 кібератак, з рекордними 271 DDoS-атаками за добу та 362 хакерськими атаками за перші 1,5 місяці війни, більшість із яких були безуспішними та без впливу на критичну інформаційну інфраструктуру.

Найбільше атак піддаються державні та місцеві органи влади, сектори безпеки та оборони, бізнес-організації в різних сферах діяльності, фінансовий сектор, телекомунікаційна інфраструктура та розробники програмного забезпечення, ЗМІ та ресурси, які збирають інформацію про військові злочини росії в Україні. Атаки здійснюються за допомогою фішингових електронних листів, поширення шкідливого програмного забезпечення та DDoS-атак. Більше половини всіх атак за перші 1,5 місяці війни були здійснені з метою збору інформації або поширення шкідливого коду.

Нова реальність активної інформаційної війни у 2021-2022 роках змушує всі організації, незалежно від розміру та сфери діяльності, комерційної чи державної форми власності, вивчати можливості захисту, інвестуючи в новітні технології «кіберзброї».

Під час воєнного стану кібербезпека стала особливо важливою для організацій будь-якого розміру та галузей. Фішингові електронні листи, злом облікових записів і викрадення даних, програми, які блокують доступ, є факторами, які підривають обороноздатність і економіку нації. Тому стратегічним завданням національних інституцій та організацій є завчасне якісне виконання роботи з кіберзахисту. Захист IT-систем за допомогою сучасних інструментів зрештою допомагає зберегти важливу інформацію, час та репутацію. У глобальному масштабі кібертероризм зростає, і питання захисту інформаційних ресурсів стало пріоритетним.

В Україні державні органи та організації для захисту інформації від злочинців все більше залучають нових постачальників рішень кіберзахисту таких як Barracuda, Fortinet, Commvault.

DoS- і DDoS-атаки діють за схожим принципом – обидві надсилають велику кількість запитів на сервер, через що атакований ресурс "зависає" без можливості обробки даних. В свою чергу DoS-атаки здійснюються з одного хосту та проти різних мереж, тоді як DDoS-атаки розподіляються та виконуються з мереж ботів (груп комп'ютерів, смартфонів, які фізично не підключені один до одного).

Для запобігання DDoS-атакам пропонується багаторівневий захист від цільового шкідливого трафіку – сервіс AntiDDoS. Він заснований на рішенні FortiDDoS від розробника Fortinet. AntiDDoS працює в інформаційній системі доступу до інтернету, контролюючи структуру трафіку до клієнтських підмереж (ресурсів). Як тільки система виявляє відхилення від дозволеного трафіку, вона автоматично спрямовується на очищення перед надходженням до клієнта.

AntiDDoS захищає від нових типів відомих і невідомих атак. Рішення просте в розгортанні та використанні та містить комплексні інструменти аналізу й складання звітів.

Нещодавно до сервісної системи боротьби з кіберзагрозами було додано ще одне програмне рішення від Commvault, однієї з провідних американських компаній-розробників, яке дозволяє захищати важливу корпоративну інформацію вашої компанії, резервне копіювання та відновлення. Це особливо важливо з огляду на збільшення кількості кібератак на державні установи та бізнес в умовах воєнного часу.

Commvault є новатором в управлінні даними, розробленим спеціально для прогнозування загроз і підтримки широкого спектру робочих навантажень у сучасних локальних, хмарних і віртуальних середовищах. Даний сервіс дозволяє використовувати його в наступних основних сценаріях:

1. Безпека даних. Багаторівневий підхід до захисту даних, швидкий автоматизований та цілеспрямований збір усіх даних для ідентифікації необхідних електронних листів, документів та всієї інформації, що зберігається в електронному вигляді.

2. Резервне копіювання даних і аварійне відновлення. Функції програмного забезпечення дозволяють:

забезпечити доступність даних для всіх робочих навантажень у хмарному, віртуальному та локальному середовищах;

виконувати реплікацію даних і аварійне відновлення для забезпечення безперервності та відновлення бізнесу в локальних і хмарних середовищах, а також створювати звіти про відповідність;

оптимізувати зберігання файлів шляхом передачі та консолідації даних, усунення зайвих даних і зменшення витрат і ризиків, пов'язаних із зберіганням;

забезпечувати захист даних корпоративного рівня.

Рішення має єдиний інтуїтивно зрозумілий веб-інтерфейс для гнучкого керування всіма засобами захисту, тому користувачі можуть легко та зручно розгорнути його та використовувати всі сервіси, а клієнти можуть отримати кращий користувацький досвід завдяки використанню штучного інтелекту та машинного навчання.

Розвиток та широке використання інноваційних інформаційних та телекомунікаційних технологій сприяли появі додаткових завдань щодо забезпечення кібербезпеки. З метою упередження деструктивної інформаційної діяльності, блокування передумов до нанесення шкоди інформаційній безпеці держави важливо, щоб усі пропоновані рішення для кіберзахисту були доступні будь-якій компанії, незалежно від галузі, форми власності чи розміру: державні установи, банки, фінансові організації, IT-бізнес, галузі, компанії, що обробляють персональні дані, сервісні компанії, роздрібна торгівля, стартапи тощо. Залежно від потреб і пріоритетів компанії, кожне рішення може бути запропоноване окремо або в поєднанні з іншими інструментами кібербезпеки, які не тільки допомагають захистити та забезпечити інформаційну безпеку, але й оптимізувати інфраструктуру.

к.ю.н. Неня О.В.(ДНДІ МВС України)
к.т.н. Фесенко М.А.(ДНДІ МВС України)
к.т.н. Березненко Н.М. (ДНДІ МВС України)

АНАЛІЗ СУЧАСНИХ СИСТЕМ ПРОТИДРОННОЇ ОБОРОНИ

Сучасні військові конфлікти мають свої особливості, які обумовлені зростанням ролі і значення засобів розвідки, спостереження, передачі даних,перенесення вантажів, а також завдавання ударів по скупченню техніки та артилерійським засобам тощо. Для виконання перелічених завдань все частіше застосовують автономні пристрої (обладнання), а саме – безпілотні літальні апарати (БПЛА) або «дрони».

На теперішньому етапі розвитку військових технологій цей напрям став найбільш пріоритетним. Провідні країни світу, такі як, США, Японія, Китай, Великобританія, Туреччина активно проводять перспективні дослідження щодо розроблення (створення) різних за своїм призначенням безпілотних літальних апаратів.

Сьогодні поняття БПЛА або «дрон» включає безліч технологічних об'єктів: від саморобних «камер з пропелерами і батарейкою» до дорогих стратегічних безпілотників вартістю 140 мільйонів доларів.

За визначенням експертів, причини бурхливого розвитку безпілотних засобів різні, основними з яких є: відсутність на борту льотчика, завдяки чому БПЛА можна використовувати для вирішення складних завдань, які пов'язані з ризиком для життя пілота. Більш того, безпілотному літальному апарату не потрібні системи життєзабезпечення екіпажу, що дозволяє значно зменшити вагу апарату і розмістити додаткове обладнання або озброєння.

З розвитком БПЛА на сьогоднішній день існує проблема використання їх позазаборонених цілях (наприклад, завдавання ударів по об'єктах цивільної інфроструктури).. Чим високотехнологічніший БПЛА, тим складніше протистояти йому без спеціального обладнання (засобів, систем).

Виробники систем протидії БПЛА постійно шукають найбільш ефективнірішення цієї проблеми. Розглянемо більш пріоритетні серед них.

Компанія Fortem з США використовує один із способів боротьби з літаючими порушниками і розробила дрона-перехоплювача під назвою DroneHunter. Він ловить невеликі безпілотники за допомогою гармати, що стріляє сіттю, яка летить зі швидкістю до 128 км/год і обплутує цілі на відстані до 7,6 метра [1]. DroneHunter ефективно і повністю автономно виявляє несанкціоновані безпілотники за допомогою вбудованого радара TrueView, який самостійно переслідує, обстрілює і захоплює літальні апарати, а потім переміщує їх, без пошкоджень.

З огляду на загрозу, яку можуть представляти літаючі машини в бойових умовах, військовим необхідно мати змогу їх знешкоджувати із землі. Компанія OpenWorksEngineering розробила систему SkyWall 300, що являє собою рушницю, з якої за допомогою стиснутого повітря вистрілює снаряд з сіттю, що заплутує «дрон» і збиває його на землю. SkyWall 300 може уражати об'єкти, які рухаються зі швидкістю до 180 км/год, на відстані до 300 метрів. Система оснащена парашутом, який акуратно спускає уражену ціль. Вона працює автоматично, її можна встановлювати на різні транспортні засоби. Втім, за необхідності, передбачається і встановлення інтерфейсу для віддаленого управління цією системою вручну [2].

Компанія Dedrone розробила ручну гвинтівку DedroneDefender, яка «стріляє» радіосигналами, що «заглушають» найпоширеніші частоти радіоуправління БПЛА в межах 400 метрів. В результаті зв'язок з оператором переривається, а безпілотники переходять в режим безпеки (зависаючі у повітрі або опускаються на землю) [3]. Якщо ж БПЛА автономно продовжує рух на базу або через заздалегідь встановлені точки, військовий може перевести гвинтівку в режим блокування GPS. Таким чином «дрони» можна повністю знешкоджувати і захоплювати до того, як вони встигли зібрати важливі розвіддані.

Під час сьогоднішньої військової агресії РФ Збройні Сили України використовують комплекси протидії «дронам» EDM4S, розроблені литовською компанією NT-Servise. Їх ефективність досягається шляхом придушення сигналів керування, відео і навігації. Комплекс цілком мобільний і готовий до використання натисканням однієї кнопки (вмикання). EDM4S включає в себе корпус рушниці, спрямовані антени, РЧ-модулі, акумулятор, голографічний або оптичний приціл. Час роботи акумулятора становить до однієї години. Крім того, обладнання може працювати й від адаптера змінного струму. Маса комплексу становить 6 кг, розміри – 250x350x900 мм [4].

Компанією BlueHalo (США) розроблена сучасна система протиповітряної оборони та протидії БПЛА – Titan C-UAS, яка використовує штучний інтелект і машинне навчання. Система складається з антенного блоку і пульта управління, є малогабаритною (її вага становить близько 9 кг), розробленою для стаціонарної, мобільної або пішої експлуатації. Така система здатна працювати при температурі до - 20°С, впоратися з групою (кількома) БПЛА одночасно [5]. Інформація про кожен «дрон» передається оператору в режимі реального часу. Titan C-UAS ідентифікує внутрішню ціль і автоматично вирішує, що з нею робити – приземлити або змусити повернутися до місця запуску. Радіус виявлення БПЛА становить 3 км, а для застосування контрзаходів комплексу Titan C-UAS потрібно 1,5 км. Іншою перевагою комплексу Titan C-UAS є можливість його застосування у міських умовах.

Одною з найефективніших систем протиповітряної оборони є ізраїльська система від компанії SmartShooter [6]. Ця система управління вогнем, по суті розумний приціл, який виявляє цілі за допомогою радара, а потім дуже точно визначає тип «дрона» та його місцезнаходження. Це допомагає збити БПЛА за допомогою стрілецької зброї. Штучний інтелект SmartShooter працює за принципом Oneshot – onehit (один постріл – одне влучення).

SmartShooter має двоядерний комп'ютер зі складною балістичною обробкою, що може розпізнавати, відстежувати та вражати повітряні (дрони/БПЛА) та наземні цілі з високою точністю. Управління SmartShooter здійснюється за допомогою штучного інтелекту та передової радарної системи. Виробник продовжує інтегрувати цю технологію в різні типи озброєння, наприклад, гвинтівки, безпілотний наземний транспорт тощо.

Боротися з ворожими квадрокоптерами-розвідниками (БПЛА) допомагають подібні до перелічених вище засобів (пристроїв), які виробляються і в Україні. Наприклад, компанією Kvertus. розроблена антидронова рушниця, наприклад, моделі KVSG-6. Пристрій придушує канали керування «дроном», що призводить до його вимушеної посадки. За даними виробника, радіус дії KVSG-6 – до 3 км, тривалість безперервної роботи – 30 хв. Для примусової посадки «дрона» його потрібно безперервно «заглушати» упродовж однієї-трьох хвилин. Кут променя «глушника» – до 30 градусів, тобто для вдалого «пострілу» навички снайпера не обов'язкові [7]. Компанією «Укрспецтехніка» розроблений мобільний протидронний комплекс, здатний ефективно нейтралізувати групові нальоти БПЛА. Такий комплекс здатний нейтралізувати БПЛА відстанню до 2 км. Система обладнана автономним живленням до 8 годин безперервної роботи[8]. В напрямку виготовлення БПЛА і засобів оборони проти них працюють десятки й інших українських виробників.

Таким чином, в даній публікації розглянуті найбільш цікаві та значимі на нашу думку системи протидронної оборони, які набувають активного поширення в світі, а також в Україні. Використання їх забезпечить більш високий рівень безпеки та захисту військових, цивільних об'єктів і осіб від уражень від БПЛА різної потужності та призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

1. В США представили новое средство против БПЛА, способное одолеть дроныShahed-136. URL: https://focus.ua/digital/532842-v-ssha-predstavili-novoe-sredstvo-protiv-bpla-sposobnoe-odolet-drony-shahed-136-video (дата звернення 12.11.22).

2. Гвинтівкисистеми "антидрон" в Україні та світі. URL:https://defence-ua.com/weapon_and_tech/gvintivki_sistemi_antidron_v_ukrajini_ta_sviti-402.html (дата звернення 12.11.22).

3. Щовідомо про литовськуантидроновурушницю та схожу українськурозробкуURL: https://armyinform.com.ua/2021/10/06/shho-vidomo-pro-lytovsku-antydronovu-rushnyczyu-ta-shozhu-ukrayinsku-rozrobku/(дата звернення 12.11.22).

4. Пневмобазука» поможет ловить дроны. URL:https://warspot.ru/5518-pnevmobazuka-pomozhet-lovit-drony.(дата звернення 12.11.22).

5. Антидроновая система Titan C-UAS: искусственный интеллект против иранских «мопедов». URL: https://itc.ua/articles/antidronovaya-sistema-titan-c-uas-iskusstvennyj-intellekt-protiv-iranskih-mopedov/] (дата звернення 12.11.22).

6. Помогут в борьбе с Shahed: характеристики систем SmartShooter.URL:https://fakty.com.ua/ru/ukraine/suspilstvo/20221027-dopomozhut-u-borotbi-z-shahed-harakterystyky-system-smart-shooter/ (дата звернення 12.11.22).

7. Вони "приземляють" 99% дронів: історіястворенняукраїнськоїантидрон-рушниці. URL:https://www.epravda.com.ua/publications/2022/06/8/687925/.

8.Мобільний комплекс наземної розвідки "ДЖЕБ". URL:https://www. news. obozrevatel.com/ukr/technology(дата звернення 12.11.22).

к.т.н. Овсянніков В.В. (ВІТІ ім. Героїв Крут)
Черниш Ю.О. (ВІТІ ім. Героїв Крут)
Фомкін Д.В. (ВІТІ ім. Героїв Крут)
Гаврилюк О.Г. (ВІТІ ім. Героїв Крут)

АНАТОМІЯ DDOS-АТАК ТА МЕТОДИ ЗАХИСТУ

Актуальність.Активний перехід робочих сервісів та сховищ даних в онлайн-середовище став невід'ємною частиною сучасного бізнесу та ведення стартапів. При цьому робота онлайн-продуктів, використання ЦОД та ведення бізнесу в цілому найчастіше піддається DDoS-атакам, які роблять системи недоступними для користувачів та власників ресурсів.

У 4 кварталі 2021 року був досягнений своєрідний рекорд за ростом кількості DDoS-атак – «Лабораторія Касперського» відзначила їх збільшення в порівняннііз попереднім кварталом на 52% і 4,5 рази – в порівнянні з минулим роком. Особливо постраждала медіа сфера, бізнес та фінансові послуги. Це було зумовлено змінами у глобальній економіці, що були викликані пандемією коронавірусу.

Постановка задачі. З початком війни такі атаки стали масштабнішими та агресивнішими, а в деяких випадках інструментом відповіді з нашої сторони. Ми маємо знати, розуміти основні принципи дії та механізми захисту від таких кібератак.

Основні положення.

Що ж таке DDoS? Ви багато разів чули цей термін, і певно у вас вже склалося розуміння про DDoS.

В більшості випадків, DDoS – це атака, яка проводиться з метою впливу на ресурси, які можливо якимось чином використати, зламати, пошкодити, ускладнити їх використання ті ін. Наприклад, паралізувати роботу додатку, перевантажити канали зв'язку, створити загрозу для систем та комплексів захисту периметру мережі (Firewal,IPS\ISD та ін.)

Існує кілька мотивів. Для кіберзлочинців це,якправило, заробляння грошей напродажі DDoS-атак якпослуги, шантажування потенційних жертв, щобвони сплатили викуп, хактивізм абоспосіб недобросовісної боротьби зконкурентами.

Під час більш складних операцій зловмисники часто використовують DDoS-атаки якодин ізінструментів длявідволікання відінших, більш серйозних видів діяльності, наприклад, кібершпигунства такіберсаботажу.

Основні категорії, які характеризують DDoSактивності.

Перший і який часто спостерігається клас DDoS – це велика кількість «сміттєвого» трафіку, який заповнює канали зв'язку та перевантажує обладнання. Такі атаки спостерігаються з великим капасіті швидкості та пакетів bpspps, легко помітні по трафіку і зазвичай довгим терміном дії. Це частина DDoS атак, яка характеризується терміном як Volymetric. Це можуть бути атаки типу Reflection\AmplificationDNS\NTP. Без сумніву, такий вид атак завдає чимало проблем для організацій та інформаційно-комунікаційних систем та мереж які не підготовлені і не мають спеціалізованих інструментів захисту.

Другий який теж досить часто має місце набагато небезпечніші та складніші атаки – це атаки рівня додатків. Їх метою є конкретний додаток, особливості його слабких місць та вразливостей. Найрозповсюджений варіант – це, наприклад, атаки типу slowloris – в основному атакує веб сервери, там немає ніякого трафіку, частіше за все – це мінімальні запити, які шляхом впливу на обробник, тримають відкритим з'єднання, змушуючи сервер постійно очікувати запити і тим самим перевантажують його. По своїй суті, ця атака спрямована на виснаження ресурсних потужностей жертви. В результаті ми отримуємо помилку 404 – сервер недоступний, яку часто можна спостерігати при відвідуванні якогось веб-ресурсу.

Третій, специфічний і цілеспрямований цілий клас точкових атак, це атаки типу Stateexhaustion – це не менш небезпечні атаки ніж попередні,а іноді досить небезпечні,

метою яких є системи захисту периметру, частіше за все, файєрволи. Тобто не доходячи до додатків атакують statefull пристрої, файєрвол,vpnконцентратор тощо. Ці атаки можуть бути не одразу помітні по трафіку і цілком легітимні з точки зору поведінки або дії. Тому часто замовники розуміють що сталося, коли вже зловмисник проник за периметр.

Статистика показує, що в основному атаки не часто використовують якийсь конкретний критерій 1, 2 або 3, як правило, це комбінація цих пунктів, тобто ми має справу з мультивекторними атаками, атаки які мають змінний вектор впливу на мережу. Це комбінації тих чи інших прийомів та впливів на інфраструктуру, простіше кажучи це розвідка і дія одночасно. Якщо Volumetric не дав результатів, переходимо на інший вид, або коригуємо комбінації атак в залежності від стану жертви.

Часто буває ,що так би мовить, простий flood, атаки типу Volymetric – це насправді прикриття, суть задачі не втому, щоб забити Вам канал або залити флудом, ціль – проникнути, пошкодити, вкрасти, видозмінити щось,тощо. Для прикладу, усі чули про атаку типу BlackEnergy, вона мала місце на нашу енергетичну інфраструктуру де чітко спостерігались як окремі типи DDoS так і її комбінації, і вони мали успіх для зловмисників. Є багато таких прикладів і історій в яких зловмисники здійснили свої задуми використовуючи прийоми мультивекторності.

Як захиститись?Організаціям, які мають обмежені ресурси, наприклад, недостатню пропускну здатність або відсутність додаткового обладнання, може бути складно перешкоджати DDoS-атакам. Однак існують заходи безпеки, які дозволяють навіть малим та середнім компаніям підвищити рівень захисту:

- відстежуйте мережевий трафікта навчіться виявляти аномалії в Інтернет-трафіку,таким чином, ви матимете можливість виявляти та своєчасно блокувати фіктивні запити;
- створіть план аварійного відновлення навипадокDDoS-атаки на вебсайт абосистему,наприклад, підготуйте резервні сервери, вебсайт таальтернативні канали зв'язку;
- проаналізуйте можливість міграції до хмари,цей крок не усуне загрозу, однак допоможе зменшити імовірність атак завдяки вищій пропускній здатності та стійкості хмарної інфраструктури.

Якщо ваша організація вже стала жертвою DDoS-атаки або перебуває в групі ризику, подумайте провикористання сервісів захисту від DoS та DDoS, які можуть допомогти зменшити негативні наслідки атаки.

Не дайте корпоративним пристроям стати частиною ботнет-мережі, яка може сприяти DDoS-атаці.

Важливо використовувати лише ліцензований софт, оновлювати ключі безпеки, а також час від часу перевіряти на наявність шкідливих програм.

Переконайтеся, що співробітники дотримуються правил кібергігієни, своєчасно оновлюйте всі пристрої та програмне забезпечення, а також забезпечте надійний захист пристроїв завдяки багаторівневим рішенням з безпеки.

Висновок. Говорячи про DDoS атаки, питання не в тому, чи будете ви атаковані, питання лише в тому коли та в який спосіб.

Можна відзначити, що витрати на DDoS атаку з боку зловмисника абсолютно незрівнянні з втратами тих організацій, які піддаються таким атакам. Можливо раніше, колись дуже давно, це (організація DDoS атак) було витратно, зараз – це дуже невеликі витрати, а наслідки від них непрогнозовані.Саме тому кожен повинен запитати себе: «Що буде, якщо моя органзація буде атакована? Які інструменти у мене є і як я зможу знівелювати наслідки тієї або іншої активності зловмисників.

Які фінансові та репутаційні втрати будуть вас спіткати? А якщо говорити ще простіше: скільки вам буде коштувати така активність зловмисників.

Створюйте багаторівневий надійний захист своїх систем та не нехтуйте основними правилами безпеки.

Ольшанський В.В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ СИСТЕМ РАДІОЗВ'ЯЗКУ ЗА ПОКАЗНИКАМИ ЕФЕКТИВНОСТІ

Сучасні системи військового радіозв'язку функціонують в складних умовах, що обумовлено дефіцитом радіочастотного ресурсу, обмеженими обчислювальними ресурсами та впливом засобів радіоелектронного подавлення супротивника. На даний час для оцінки систем військового радіозв'язку розроблено безліч показників оцінки їх ефективності, проте їх застосування обумовлено рядом обмежень, яка полягає в тому, що показники, які мають високу точність як правило не використовуються в зв'язку з високою їх обчислювальною складністю, а ті показники, що мають прийнятну обчислювальну складність мають низьку точність оцінювання.

Для кількісної оцінки ефективності систем радіозв'язку необхідно мати кількісні показники ефективності. У ранніх роботах по теорії передачі інформації, як показник ефективності, використовувалась швидкість передачі інформації. Однак така міра оцінки не є задовільною, оскільки вона враховує лише витрати часу й не враховує затрат смуги частот і потужності сигналу.

У доповіді розглянуто аналіз систем радіозв'язку за показниками ефективності. Встановлено, що сучасні складні системи радіозв'язку не завжди можуть бути вичерпно охарактеризовані одним показником. Оцінка за декількома показниками є більше повною й більше конкретною і дозволяє охарактеризувати різні властивості системи. Оптимізація системи передачі в цілому, тобто з урахуванням пристроїв кодування й декодування, здійснюється на основі теорії інформації.

Найбільш загальною оцінкою ефективності системи зв'язку є коефіцієнт використання каналу за пропускною здатністю (інформаційна ефективність). Для забезпечення заданої швидкості передачі інформації та заданої вірогідності доводиться витрачати деяку потужність сигналу і займати певну смугу частот у каналі зв'язку. Яка потужність і яка смуга частот при цьому знадобиться, залежить від системи зв'язку, що використовується.

Ефективність системи передачі інформації оцінюється коефіцієнтом використання потужності сигналу (енергетичною ефективністю) і коефіцієнтом використання смуги частот каналу (частотною ефективністю). Підвищення частотної ефективності вимагає збільшення енергетичних витрат (зниження енергетичної ефективності).

При високих вимогах до вірності передачі доцільним стає застосування завадостійких кодів, які дозволяють підвищити енергетичну ефективність в обмін на зниження питомої швидкості передачі інформації. Одночасна вимога високої швидкості та вірності передачі інформації в умовах обмеженого частотного і енергетичного ресурсу може бути виконане при спільному використанні багатопозиційних сигналів і потужних завадостійких кодів.

Для оцінки енергетичної ефективності систем радіозв'язку доцільно застосовувати коефіцієнт використання потужності сигналу. Переваги підвищення енергетичної ефективності очевидні: мінімізація потужності випромінювання передавача, покращення електромагнітної сумісності радіоелектронних засобів, підвищення прихованості передачі інформації, мінімізація енергоспоживання.

Проведений аналіз систем радіозв'язку за показниками ефективності, показує, що сучасні складні системи радіозв'язку не завжди можуть бути вичерпно охарактеризовані одним показником. Оцінка за декількома показниками є більше повною й більше конкретною і дозволяє охарактеризувати різні властивості системи.

Для оцінки ефективності систем радіозв'язку доцільно застосувати коефіцієнт використання потужності сигналу. Величина коефіцієнта використання потужності сигналу залежить від виду сигналу, виду та інтенсивності завади.

Напрямком подальших досліджень є розробка математичної моделі спотворення сигналу при впливі навмисних завад.

Опалинський В.Б. (НАСВ)

ПЕРЕВАГИ СИСТЕМ КІБЕРЗАХИСТУ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

Завдяки розвитку інформаційних технологій та Інтернету загалом виникають проблеми, пов'язані із забезпеченням кібербезпеки користувачів. Мережа Інтернет з наукового інструментарію перетворилася на одну з головних інфраструктур інформаційної спільноти світу. Всесвітню мережу застосовують як уряди для інформування громадян, так і компанії для обміну інформації між своїми підрозділами, партнерами та клієнтами для підвищення ефективності бізнес-діяльності. Навчальні та наукові заклади використовують мережу для дистанційного навчання та як платформу для співпраці, та для швидкого обміну інформацією.

Але зі зростанням і поширенням Інтернет-мереж зростала і кількість атак. Не так давно утворився термін «кібернетичний тероризм», тобто загрози стали організованими та навіть спрямованими на ІТ-інфраструктури деяких держав. Так, захищеність Інтернет-мереж стала питанням безпеки не тільки бізнесу, але і держав. Тож, дослідження шляхів захисту від кібератак у мережі є важливим та актуальним. За останні роки комп'ютерні та мережеві технології розвинулися, збільшилась як кількість користувачів, так і складність побудови сервісів для їх обслуговування. Але разом з розширенням систем з'явились і вразливості різного роду. Навіть фактор зростання мобільності користувачів значно ускладнює побудову сервісів та їх захист, адже це робить їх поведінку непередбачуваною, бо зі зміною точки підключення зміниться і конфігурація мережі, тоді усі зібрані раніше характеристики стануть недостовірними. Але і сама поява нових вразливостей і типів атак впливає на складність побудови сервісів.

Нинішній розвиток вказує на те, що подальшим напрямком буде створення мережі з інтелектуальними компонентами, що дозволить досягти більшої автономності та адаптивності, стане можливим, завдяки взаємодії системи захисту з цими компонентами, оцінювати кіберзагрози і обирати ефективні методи виявлення і боротьби з ними. Як висновок, є необхідність в розробці систем виявлення і захисту, які могли б задовольнити такі вимоги:

– ефективність функціонування: висока надійність виявлення, швидкість роботи, стійкість до фальшивих виявлень;

– масштабованість: розширення або зміна конфігурації системи мають автоматично враховуватися;

– адаптивність: поява нових видів атак або зміна характеристик роботи не має призводити до необхідності перепрограмування системи. Інтелектуальні інформаційні системи поділяють на групи, в залежності від концепції, на якій заснована така система, а саме: статистичний аналіз даних; засоби інтелектуалізації доступу до бази даних; евристичне вирішення завдань діагностики та прогнозування на основі застосування експертних систем; аналіз та прогнозування на основі використання нейронних мереж, а також баз знань прецедентів; програмні засоби динамічного планування на основі case-технологій тощо. Та, як базис для створення систем кіберзахисту мереж найбільш доцільним є застосування інтелектуальних агентів, що користуються методами статистичного аналізу та теорії ігор. Досвід використання таких систем описано та обґрунтовано у багатьох роботах.

Така система зможе планувати протидії зловмисним діям завдяки базі стратегій, отриманій при аналітичному моделюванні взаємодії, та зібраним даним. Вивчення інтелектуальних моделей кіберзахисту мереж дозволить чинити ефективну протидію та передбачувати можливі наслідки. Таке моделювання можливе завдяки ігровому аналізу, адже модуляція будується завдяки конфліктній взаємодії між нападниками та системою захисту. Складність таких систем викликає необхідність введення нових припущень, ідеалізації руху, аналіз динаміки, ідеалізацію керувань конфліктуючих груп, та визначення прийнятих стратегій захисту. Ці припущення є складними науковими проблемами, вирішення яких створить передумови для успішної розробки та функціонування інтелектуальних систем кіберзахисту.

Османов Р.Н. (ВІТІ ім. Героїв Крут)
к.т.н. Штаненко С.С. (ВІТІ ім. Героїв Крут)

ІНТЕГРАЛЬНІ СХЕМИ З ПРОГРАМОВАНОЮ СТРУКТУРОЮ ЯК ОСНОВА ПРОЄКТУВАННЯ СУЧАСНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Успіхи в галузі інтегральних технологій, досягнуті за останні десятиліття, призвели до створення великих/надвеликих інтегральних схем (ВІС/НВІС), що містять сотні тисяч елементів на одному кристалі. Однак поява ВІС/НВІС породила дуже серйозну проблему, яка пов'язана із синтезом цифрових пристроїв на схемах з такою великою кількістю елементів.

Першим і досить природним рішенням цієї проблеми стало виготовлення замовних схем (*ASIC – Application-SpecificIntegratedCircuit*), що розробляються щоразу спеціально для використання в конкретній радіоелектронній апаратурі. У той же час проєктування замовних ВІС/НВІС – досить тривалий і трудомісткий процес, який використовує системи автоматичногопроєктування (САПР). Тому розробка та виготовлення замовних ВІС/НВІС може бути економічно виправдана тільки при масовому виробництві радіоелектронної апаратури, в якій ці схеми застосовуються[1].

Однією з альтернатив замовним ВІС/НВІС є мікропроцесорні набори – це сукупність ВІС/НВІС, що реалізують складні функції цифрової апаратури. З цих наборів досить просто проєктуються обчислювальні системи, що отримали винятковий розвиток і знайшли широке застосування у різноманітних системах управління складними об'єктами та технологічними процесами.

Мікропроцесор є універсальним пристроєм, здатним реалізувати будь-яку логічну функцію. Однак програмна реалізація логіки управління здійснюється порівняно повільно, мікропроцесори часто не здатні забезпечити необхідну швидкодію [2]. У зв'язку з цим на сьогоднішній день широке розповсюдження отримали програмовані логічні інтегральні схеми (ПЛІС). Дані інтегральні схеми є матрицею програмованих логічних елементів з *SPLD* (*SimpleProgrammableLogicDevice*s), *CPLD* (*ComplexProgrammableLogicDevice*), *FPGA* (*Field-ProgrammableGateArray*), *FLEX* (*FlexibleLogicElementMatrix*) структурами. Характерною особливістю є те, що на відміну від звичайних цифрових мікросхем, логіка роботи ПЛІС не визначається при виготовленні, а задається за допомогою програмування (проєктування). Для програмування використовується інтегроване середовище розробки (*IDE – IntegratedDevelopmentEnvironment*), що дозволяє задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми спеціальними мовами опису апаратури, такими як *AHDL*, *VHDL*, *Verilog* тощо.

До переваг ПЛІС слід віднести [3]:

універсальність, тобто. можливість створення практично будь-якого цифрового пристрою на кристалі за наявності персонального комп'ютера та відповідних інструментальних засобів (САПР);

можливість модифікації проєктів на будь-яких стадіях розробки та в процесі експлуатації; висока швидкодія, мала споживча потужність та висока надійність, що забезпечується технологією виготовлення кристалів;

сумісність із навколишнім середовищем за рахунок можливості вибору рівнів напруги живлення та параметрів сигналів введення/виводу;

низька порівняно з ВІС/НВІС вартість реалізації проєктів за рахунок масового виробництва кристалів з регулярною структурою та невеликого часу, що витрачається на розробку проєктів та їх верифікацію.

Крім цього, вибираючи за основу ті чи інші структури ПЛІС ми маємо можливість проєктувати не тільки комбінаційні та послідовні цифрові пристрої, цифрові автомати Мілі та Мура, а й обчислювальні системи шляхом реалізації одного з рівнів проєктування: низького, блочного або високого.

Низький рівень передбачає використання мов опису апаратури *AHDL*, *VHDL*, *Verilog*, які управляють розробкою цифрового пристрою лише на рівні регістрових передач (*RTL – RegisterTransferLevel*). При цьому формуються регістри (аналогічні процесору) і визначаються логічні функції, які змінюють дані між ними.

На блочному рівні відбувається з'єднання бібліотечних програмоподібних IP-блоків (*IntellectualProperty*), які виконують певні функції для отримання потрібної функціональності системи на кристалі (*System-on-Chip*, *SoC*).

Система на кристалі або *SoC*– це обчислювальна система, архітектура якої розроблена цільовим чином для вирішення прикладної задачі або класу задач. Технологія *SoC* реалізована у вигляді комплексу функціонально спеціалізованих апаратних та програмних компонентів на базі реконфігурованої мікроелектронної платформи. Крім цього дана технологія складається з двох самостійних функціональних частин ПЛІС *FPGA* (*Field-ProgrammableGateArray* – програмована вентильна матриця) та *HPS* (*HardProcessorSystem* – жорстка процесорна система), які з'єднані між собою інтерфейсом обміну даними [4].

На високому рівні проєктування застосовуються високорівневі мови програмування *C/C++*, *System C*, *Python*, *Java*, які на рівні абстракції, тобто введенні смислових конструкцій, коротко описують структури обчислювальних систем та операції над ними. Крім цього за допомогою компіляторів та трансляторів (*HLS* для *C/C++*, *MyHDL* для *Python*, тощо) дають можливість транслювати написані блоки (структури) мовами опису апаратури *Verilog*/*VHDL* на рівень *RTL* – рівень реєстрових передач.

Крім цього слід зазначити, що стрімкий розвиток технології ПЛІС призвів до того, що в даний час вони успішно конкурують з універсальними мікропроцесорами, мікроконтролерами, сигнальними процесорами та одноплатними комп'ютерами типу *Raspberry Pi* в областях управління та високошвидкісної обробки даних, цифрової обробки сигналів, криптографії та інших областях.Це, насамперед, пов'язано з тим, що ПЛІС мають властивість реконфігурації внутрішньої структури, тобто зміна архітектурі на рівні логічних елементів, на відміну від перерахованих раніше обчислювальних пристроїв, які мають фіксовану архітектуру і фіксований набір команд.

Таким чином, можливість реконфігурації архітектурі є істотною перевагою ПЛІС при використанні в системах, де критичним фактором є безперервна працездатність. Це пов'язано з тим, що у разі відмови одного з елементів ПЛІС можна виконати реконфігурацію з метою відновлення працездатності, замінивши елемент, що відмовив, резервним або перерозподілити функції та задачі серед працездатних елементів. Тому багато провідних виробників в галузі електроніки використовують ПЛІС як співпроцесори універсальним мікропроцесорам або у вигляді додаткових модулів у багатопроцесорній системі. Всі ці характеристики ПЛІС в кінцевому підсумку дозволяють проєктувати високонадійні, відмовостійкі, живучі, функціонально стійкі обчислювальні системи, здатні функціонувати в умовах як ненавмисного так і навмисного впливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хорошевский В.Г. Архитектура вычислительных систем.: Учеб. пособие. 2-е изд., перераб. и доп. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 520 с.

2. *VaibbhavTaraate. PLD Based Designwith VHDL RTL Design, Synthesisand Implementation, Springer Nature Singapore Pte Ltd, p. 423, 2017.*

3. Каляев И.А. Семейство реконфигурируемых вычислительных систем с высокой реальной производительностью / И. А. Каляев, И.И. Левин, Выч. мет. программирование, №10:1 (2009). С. 61 – 68.

4. Уваров С.С. Проектирование реконфигурируемых отказоустойчивых систем на ПЛИС с резервированием на уровне ячеек. – Автоматика и телемеханика, 2007, № 9.С. 176–189.

Остапчук В. М. (ВІТІ ім. Героїв Крут)
Величко В.П. (ВІТІ ім. Героїв Крут)

МЕТОДИКА ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ БАГАТОАНТЕННИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЗІ СПЕКТРАЛЬНО-ЕФЕКТИВНИМИ СИГНАЛАМИ В УМОВАХ ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ЧИННИКІВ

Вступ

Технологія MIMO (*Multiple Input Multiple Output* – багато входів багато виходів) знайшла практичне застосування у багатьох сучасних телекомунікаційних системах. Суть технології MIMO подібна до методу рознесеного прийому, коли на приймальному боці створюються декілька некорельованих копій сигналу за рахунок рознесення антен у просторі, за поляризацією, рознесення сигналів за частотою або у часі.

На завадозахищеність багатоантенних систем радіозв'язку впливають навмисні завади та завмирання сигналу, що виникають у ході багатопроменевого розповсюдження радіохвиль. Також одним з обмежень, технології MIMO є низька пропускна спроможність антенних каналів. З одного боку, для підвищення ефективності використання радіочастотного ресурсу та боротьби з завмираннями сигналу спільно з технологією MIMO використовуються спектрально ефективні сигнали з частотним ущільненням (*Spectrally Efficient Frequency Division Multiplexing* – SEFDM).

З іншого боку, спільне використання технології MIMO та SEFDM знижує енергетичну ефективність каналів і в свою чергу призводить до зниження завадозахищеності.

Це обумовлює необхідність пошуку нових наукових підходів, що дозволять, при заданому рівні пропускної спроможності каналів системи MIMO, забезпечити необхідний рівень завадозахищеності.

Метою дослідження є розробка методики підвищення завадозахищеності багатоантенних систем зі спектрально-ефективними сигналами спеціального призначення в умовах впливу дестабілізуючих чинників.

Виклад основного матеріалу дослідження

Методика підвищення завадозахищеності багатоантенних систем зі спектрально-ефективними сигналами спеціального призначення в умовах впливу дестабілізуючих чинників складається з наступної послідовності дій:

1. *Введення вихідних даних*. Вводяться параметри багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами. До таких параметрів відносяться: вид модуляції, розмірність ансамблю сигналів, тривалість кадру на виході демодулятора, тривалість кадру на виході декодера, швидкість коригувального коду, величина кодової відстані, тип кодеру попереднього кодування.

2. *Оцінка стану каналу*. На даному етапі за допомогою розробленого авторами методу оцінки стану каналу оцінюється стан багатопроменевого каналу та визначається його канальна матриця.

3. *Попереднє кодування*. Задача знаходження оптимальних параметрів попереднього кодування для репрезентативного набору матриць, характерного, відповідно до зібраної статистики, для даного поєднання антенної групи та вектору колокації, вирішується чисельно.

4. *Прогнозування стану каналів багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами.*

Процедуру прогнозування стану каналів багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами будемо розглядати на основі нечітких когнітивних моделей та штучної нейронної мережі.

5. *Вибір параметрів СКК*. Алгоритм вибору СКК для кожного власного каналу складається з вибору, в залежності від завадової обстановки, виду модуляції, вибору

коректувального коду і вибору маніпуляційного коду. В даній процедурі відбувається пошук оптимальної СКК за допомогою нечітких когнітивних моделей.

6. *Вибір способу обробки сигналів при прийманні.*

На даному етапі вибирається один із способів обробки сигналів в приймачі системи MIMO: детектування з максимальною правдоподібністю; приймання з мінімальною середньоквадратичною помилкою (MMSE) або так зване „сліпе" приймання сигналів. Після вибору способу обробки сигналів перевіряється виконання вимог із забезпечення заданої ймовірності помилкового приймання сигналів.

Висновки.

Запропонована методика підвищення завадозахищеності багатоантенних систем зі спектрально-ефективними сигналами спеціального призначення в умовах впливу дестабілізуючих чинників.

Сутність розробленої методики полягає у виборі значень параметрів системи MIMO та спектрально-ефективних сигналів (раціональних параметрів попереднього кодування). Також параметрів сигналів для кожного каналу системи MIMO в залежності від поточного стану передаточної характеристики каналу. Вибір здійснюється з урахуванням результатів прогнозування за критерієм мінімуму ймовірності бітової помилки при виконанні обмежень на швидкість передачі інформації.

Раціональні значення параметрів сигналу для конкретного стану каналу визначаються зі скінченної кількості допустимих варіантів, що дозволяє спростити практичну реалізацію обладнання багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами. Параметрами сигналу, значення яких визначаються при розв'язанні оптимізаційної задачі, є: параметри попереднього кодування, кількість піднесучих, параметри сигнально-кодової конструкції, метод обробки сигналів та потужність передавача.

Основними перевагами запропонованої методики є: використання комплексного показника оцінки стану каналу, що враховує більшість відомих параметрів оцінки; однозначність отриманої оцінки стану каналу; широка сфера використання (системи радіозв'язку та радіолокації); простота математичних розрахунків; підвищена оперативність оцінки стану каналу за рахунок використання теорії штучного інтелекту; можливість адаптації до сигнальної обстановки в каналі та прогнозування стану каналу; можливість синтезу оптимальної структури засобу радіозв'язку.

До недоліків запропонованої методики слід віднести:

– втрату інформативності при оцінюванні стану каналу за рахунок комплексної оцінки;

– меншу точність оцінювання за окремо взятим параметром оцінки стану каналу;

– меншу точність оцінювання на початковому етапі, що пов'язано з ненавченістю нейронної мережі та відсутністю бази сигнальної обстановки;

– методику не доцільно використовувати в системах радіозв'язку при необхідності отримання точної оцінки стану каналу за окремим показником.

Запропоновану в роботі методику доцільно використовувати при розробці програмного забезпечення для модулів (блоків) оцінки перспективних засобів радіозв'язку, які базуються на інтерфейсах відкритої архітектури версії SCA 2.2.

Одержані результати можуть бути застосовані в адаптивних прийомопередавачах багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами, що дозволить істотно підвищити їх завадозахищеність в умовах навмисних завад та селективних завмирань.

Зазначена методика дозволяє підвищити завадозахищеність каналів багатоантенних систем військового радіозв'язку зі спектрально-ефективними сигналами на 20–25 %, що підтверджується результатами моделювання.

Паламарчук Н.А. (ВІТІ ім. Героїв Крут)
Чередниченко О.Ю. (ВІТІ ім. Героїв Крут)
Паламарчук С.А. (ВІТІ ім. Героїв Крут)
Мартинюк В.В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ВІЙСЬКОВИХ КОНФЛІКТАХ

В ході останніх воєнних конфліктів в Іраку, Лівії, Сирії, Нагірному Карабасі та Україні спостерігається тенденція підвищення ефективності застосування безпілотних літальних апаратів (БпЛА) для виконання різних завдань з використанням різних підходів їхнього застосування. Роль БпЛА зростає: розвідка (дорозвідка), коригування вогню, нанесення ударів по наземних/надводних цілях, постановка радіоелектронних завад, використання в якості хибних повітряних цілей для викриття позицій сил і засобів, зокрема засобів протиповітряної оборони (ППО), придушення роботи системи ППО з метою завоювання переваги в повітрі і знищення основних засобів озброєння противника, тощо. Загалом, відбулася зміна стратегії ведення війни в частині застосування БпЛА, масове багатоетапне застосування груп відносно недорогих легких розвідувальних і розвідувально-ударних БпЛА, а також груп "БпЛА-камікадзе", так звана "тактика роїння" (swarm) – удари кількома БпЛА по одній цілі.

Як приклад, характерною рисою військового конфлікту між Вірменією і Азербайджаном в Нагірному Карабасі восени 2020 року стало масоване застосування Азербайджаном БпЛА для знищення спочатку системи ППО, а в подальшому, живої сили та озброєння сухопутних військ Вірменії. Азербайджан використовував відомі в Україні турецькі БпЛА Bayraktar TB2, ізраїльські Heron TP і Hermes, баражуючі боєприпаси "БпЛА-камікадзе" Sky Striker і Harop, тощо. Відсутність аналогічних БпЛА у Вірменії, а також слабка ППО на території конфлікту, (наявні ЗРК "Оса" і "Стріла" орієнтовані на знищення літаків та гелікоптерів і не призначені для боротьби з БпЛА), дозволила Азербайджану завоювати перевагу в повітрі (показати низьку живучість системи ППО в умовах масованого нальоту групи БпЛА), і в цілому, досягти стратегічної переваги у війні. Без застосування БПЛА в Нагірному Карабасі, вірменські системи ППО були б цілком спроможні стримувати азербайджанську авіацію [1-3].

Ситуація війни в Україні трохи інша, спостерігається більш широке застосування БпЛА з обох сторін для вирішення різних завдань (як розвідувальних, так і ударних). рф використовує як свої "Орлан-10", "Форпост-Р", "Елерон", "Куб-БЛА", "Ланцет", "Іноходець", так і БпЛА, придбані в Ірані: "Shahed-129" (Шахід-129), "Shahed-191" (Шахід-191), "Mohajer-6" (Мохаджер-6), "Mohajer-4" (Мохаджер-4), "Shahed 136" (Шахід 136) – "Герань-2" (їх характеристики та демаскуючі ознаки частково є у відкритих джерелах) [3, 6].

Останнім часом рф використовує групи "БпЛА-камікадзе" "Shahed 136" ("Герань-2") для враження військових об'єктів (в основному поза полем бою) та об'єктів критичної інфраструктури України, первинно досягла деякого успіху у руйнуванні енергетичної інфраструктури, а в подальшому, застосування всієї сукупності вогневих засобів ЗСУ дозволило успішно боротися з ними (за різними даними відсоток збиття складає ~55-85%, і щоразу покращується. Для порівняння відсоток збиття російських ракет 50-55%, інколи 80%). На думку експертів, не варто надто демонізувати цю ситуацію (з Шахідами), тому що окрім цих БпЛА, у росії є значно потужніша зброя. Також, згідно огляду американського Інституту дослідження війни *(ISW)*, використання росією БпЛА не призводить до асиметричних ефектів, як використання Україною наданих США систем *HIMARS*, і навряд чи суттєво вплине на перебіг війни, мабуть, вони використовують БпЛА сподіваючись створити нелінійні ефекти за допомогою терору. Тобто, росія застосовуючи БпЛА не отримала стратегічної переваги у війні з Україною як це очікувалося і не змінила ситуацію

на фронті, поки що йде перевірка систем ППО України на міцність (всіх наявних засобів ураження) та вичерпання їх бойового ресурсу [4, 5].

Відповідно до аналізу, який ґрунтується на відкритих джерелах, Україна витрачає на боротьбу з російськими БпЛА набагато більше коштів, ніж росія на їх "невдале" використання (виробництво/закупівлю та запуск) [3, 5].

Система ППО України поки що вистояла (хоча теж була розрахована скоріше на боротьбу з авіацією та крилатими ракетами, ніж з БпЛА), однак, подальший розвиток тактики групового застосування БпЛА істотно ускладнює умови її функціонування і занадто дорогий (позиція ефективність/вартість), що потребує модернізації. Напрямки модернізації: оновлення озброєння (засобів, комплексів та снарядів до них); створення єдиної вертикалі управління та взаємодії розрахунків системи ППО (всіх задіяних сил та засобів ураження); ведення розвідки; підвищення обізнаності бойових розрахунків та своєчасності передачі інформації.

Узагальнені рекомендації щодо комплексної протидії БпЛА рф: маскування своїх позицій; створення системи хибних та імітаційних позицій; виявлення за допомогою радарів (пеленгаторів) та збиття вогневими засобами (використання мобільних вогневих груп); протидія з використанням засобів РЕБ (глушіння GPS/системи навігації та збиття з курсу), захоплення пастками-сітками, тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жирохів М. Нагірний Карабах: як ізраїльські та турецькі безпілотники змінили хід історії // [Електронний ресурс]. 20.10.2020. URL: https://mind.ua/ru/openmind/20217213-nagornyj-karabah-kak-izrailskie-i-tureckie-bespilotniki-izmenili-hod-istorii.

2. Чередниченко О.Ю., Процюк Ю.О. Шемендюк О.В., Лебідь Є. В. Аналіз досвіду бойового застосування безпілотних літальних апаратів проти зенітно-ракетних комплексів у військовому конфлікті в Нагірному Карабасі. // Системи і технології зв'язку, інформатизації та кібербезпеки. Київ: ВІТІ № 1 (1) – 2022. – С. 114 – 121.

3. Аксенов П. Україна проти "Шахедів": як недорого та ефективно боротися з дронами-камікадзе? // [Електронний ресурс]. 20.10.2022. URL: https://www.bbc.com/russian/features-63322739.

4. Катков О. Звикаємо їздити без навігаторів. // [Електронний ресурс]. 14.10.2022. URL: https://nv.ua/ukraine/events/kak-budut-glushit-iranskie-drony-shahed-136-oborudovaniem-kotoroe-peredast-nato-ekspert-novosti-ukrainy-50276725.html.

5. Колонович К. The Guardian порахував, у скільки Україні обходиться збиття російських дронів // [Електронний ресурс]. 21.10.2022. URL: https://speka.media/the-guardian-poraxuvav-u-skilki-ukrayini-obxoditsya-zbittya-droniv-pi5zo9.

6. Коробейніков Д. Які безпілотники використовують армії Росії та України: повний список // [Електронний ресурс]. 17.10.2022. URL: https://fedpress.ru/article/3119779.

д.т.н. Пількевич І.А. (ЖВІ ім. С.П. Корольова)
к.т.н. Бойченко О.С. (ЖВІ ім. С.П. Корольова)
Лобода Р.І. (ЖВІ ім. С.П. Корольова)
Лобода В.В. (ЖВІ ім. С.П. Корольова)

ОЦІНЮВАННЯ РІВНЯ ЗНАНЬ КОРИСТУВАЧІВ ІКС

Актуальність. Захист інформації від витоку та несанкціонованого доступу в інформаційно-комунікаційних системах (ІКС) є одним з головних завдань установ щодо забезпечення ефективного виконання своїх основних функцій. На сучасному етапі розвитку інформаційних технологій захист інформації умовно поділяється на захист від зовнішніх та внутрішніх загроз. Якщо захист інформації від зовнішніх загроз має потужний технічний інструментарій, який обґрунтовано науковими дослідженнями у сфері криптографічного та технічного захисту інформації, то від внутрішніх загроз полягає в основному у виконанні організаційних заходів, які проводяться в ході створення комплексної системи захисту інформації[1].

Постановка задачі.Для захисту інформації від внутрішніх загроз розробляються модель порушника та модель загроз інформації. Перша відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії. У ході розробки моделі внутрішнього порушника враховують лише апріорні знання користувачів ІКС, а не реально оцінені. Тому існує потреба в оцінюванні рівня знань користувачів ІКС за результатами виконання ними тестових завдань. Виникнення цього важливого науково-практичного завдання обумовлено протиріччям між високими вимогами до адекватності математичної моделі внутрішнього порушника та принциповою неможливістю оцінювання його рівня знань за рахунок застосування відомих моделей, які використовують апріорні знання, що й визначає актуальність та своєчасність досліджень.

Основні положення.Для оцінювання рівня знань користувача ІКС застосовують методи та способи сучасної теорії тестів IRT (ItemResponseTheory), яка надає інструментарій для визначення рівня знань тестованого за результатами виконання ним тестових завдань, які оцінюються деякою неперервною величиною, що приймає значення з відрізка. Зв'язок між рівнем знань та виконанням тестових завдань визначається деякою нелінійною залежністю.

Відповідно до основної гіпотези теорії тестів, імовірність виконання тестового завдання є функцією латентного параметра рівня знань тестованого та латентного параметра складності тестового завдання. Під латентним параметром слід вважати властивість особистості, яка недоступна для безпосереднього спостереження.

Відповідно до математичної теорії параметричної оцінки тестових завдань, а саме математичної моделі Раша, оцінка рівня знань тестованого визначається у шкалі логітів. Логіт рівня знань – ненатуральний логарифм відношення частки правильних відповідей на осі завдання до частки неправильних.

У моделі контролю знань (логістичній моделі) наведено вимогу щодо складності завдань: одне з них вважається складнішим, ніж інше, якщо ймовірність правильної відповіді на нього менша, незалежно від виконавця.

Недоліком наведених вище моделей є відсутність оцінки якості відповіді на завдання. Тому метою дослідження є розробка математичної моделі оцінювання рівня знань користувачів ІКС за допомогою шкали результатів виконання тесту.

Методика оцінювання рівня знань тестованого за результатами виконання тестових завдань включає такі кроки:

1. Розрахунок складності тесту.
2. Розрахунок якості відповіді.
3. Розрахунок імовірності правильної відповіді.
4. Розрахунок рівня відповіді.

5. Розрахунок частки правильних відповідей.

6. Вибір шкали результатів виконання тестів та розрахунок її числових значень.

Розробка математичної моделі оцінювання рівня знань користувачів.Для оцінювання рівня знань тестованого за результатами виконання тестових завдань визначено такі кроки:

1. Розрахунок складності тесту (complexityofthetest). Складність тесту характеризується кількістю завдань різного рівня складності та визначає максимальну оцінку, яку може отримати тестований за умови надання всіх правильних відповідей на завдання тесту.

2. Розрахунок якості відповіді (qualityofanswer). Якість відповіді є неперервною випадковою величиною, розподіленою на проміжку [0…1], що характеризує повноту правильної відповіді.

3. Розрахунок імовірності правильної відповіді (probabilityofthecorrectanswer). Імовірність правильної відповіді залежить від кількості рівнів складності завдань, її визначають таким співвідношенням.

4. Розрахунок рівня відповіді (answerlevel). Рівень відповіді є неперервною випадковою величиною, розподіленою на проміжку [0…1], що характеризує повноту правильної відповіді, отриманої на завдання з відповідним рівнем складності. При цьому рівень відповіді враховує не ймовірність правильної відповіді на завдання, а складність самого завдання.

5. Розрахунок частки правильних відповідей (shareofcorrectanswers). Частка правильних відповідей є неперервною випадковою величиною, розподіленою на проміжку [0…1], що характеризує рівень знань на основі якості відповідей, отриманих на завдання різного рівня складності.

6. Вибір шкали результатів виконання тестів та розрахунок її числових значень. Межі шкали результатів виконання тесту залежать від кількості якісних показників оцінки результатів виконання тестів.

Для перевірки розробленої моделі розглянуто приклад оцінювання рівня знань користувачів ІКС. Під час оцінювання було використано тест, який складався з 30 завдань чотирьох рівнів складності та з чотирма варіантами відповідей на кожне завдання. Тест має 10 завдань 4-го (найнижчого) рівня складності; 10 завдань 3-го (середнього) рівня складності; 6 завдань 2-го (високого) рівня складності; 4 завдання 1-го (найвищого) рівня складності.

В роботі приведено результати перевірки розробленої моделі при заданих вихідних даних.

Висновок.Таким чином, при оцінюванні рівня знань користувачів ІКС враховується рівень складності завдань тесту, а також якість відповіді. Отримані результати свідчать, що вірні відповіді на тести більш високого рівня дають більш високу оцінку знань користувача.

Математична модель оцінювання рівня знань користувачів ІКС може бути використана для оцінювання рівня складності тесту, так і рівня знань тестованого. Вона враховує не апріорні (раніше не відомі) знання, а ті, рівень яких оцінено за допомогою тестів із відповідним рівнем складності та якістю відповіді на завдання.

Результати виконання тестів надають якісну оцінку рівня знань користувачів ІКС і далі можуть бути використані для розробки моделі внутрішнього порушника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки Українивід 28.04.1999 № 22. URL:http://dsszzi.gov.ua/dsszzi/doccatalog/ document?id =106340 (дата звернення: 12.05.2020).

Площик А.С. (НАДПСУ)

МОЖЛИВОСТІ ВИКОРИСТАННЯ ВИМІРЮВАЧА ВІДСТАНІ З ПЕРЕДАЧЕЮ ДАНИХ ПО РАДІОКАНАЛУ В РОБОТОТЕХНІЧНИХ КОМПЛЕКСАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ.

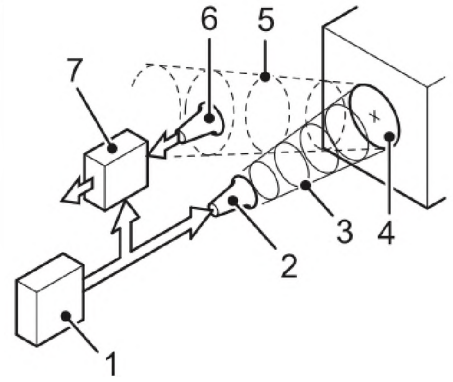
Актуальність. Розглядається можливість застосування вимірювача відстані на Arduino з передачею даних по радіоканалу. В даний час існує безліч подібних пристроїв вимірювання відстані з передачею даних на ЕОМ, або на мобільний пристрій на основі технології Bluetooth або WiFi. Одним з основних недоліків такого способу передачі даних є те, що для прийому даних вимірювання необхідно використовувати додатковий пристрій зі встановленим спеціальним програмним забезпеченням, що приводить до підвищення ціни цих приладів.

Постановка задачі. В цій роботі буде запропоновано вирішення цих недоліків та ідея розробки повністю незалежного пристрою.

Найкращим методом рішення поставлених цілей буде розробка двох приладів: окремо вимірювача відстані і окремо пристрою для відображення даних. Тобто, для досягнення мети, необхідно розробити пристрій, який буде вимірювати відстань, обробляти вхідні дані з датчику відстані, готувати та передавати дані до передачі по радіоканалу та пристрій, який буде приймати такі дані, та відображати їх на дисплеї.

Основні положення. Провівши порівняння можливих методів вимірювання дальності, та проаналізувавши їх переваги та недоліки було прийнято рішення використовувати датчик відстані на основі ультразвукової технології. Однією з основних переваг таких датчиків є їх простота та відмовостійкість. Серед доступних датчиків такого типу – найпопулярнішим є готовий модуль HC-SR04. Даний модуль працює за принципом ехолокації, тобто рахує час проходження ультразвуку від випромінювача до приймача.

Для оцінки правильного вибору прийнятого рішення варто розглянути принцип роботи датчика відстані на рисунку 1.



Умовні позначення на рисунку 1:
1.Генератор імпульсів
2.Ультразвуковий випромінювач
3.Випромінені ультразвукові імпульси
4.Об'єкт вимірювання
5.Відбиті ультразвукові імпульси
6.Приймач відбитих ультразвукових імпульсів
7.Обчислювач

Рис.1 - Візуальна схема роботи модуля HC-SR04

Генератор імпульсів (1) формує 8 імпульсів з частотою 40 кГц та передає їх на випромінювач (2) чим запускає вбудований таймер в обчислювачі(7). Ультразвукова хвиля досягає об'єкта, відстань до якого необхідно виміряти відстань. Хвиля від нього відбивається та досягає приймача (6). Приймач перетворює відбиту ультразвукову хвилю в електричний сигнал та передає його в обчислювач(7). Обчислювач зупиняє вбудований таймер, і на основі його виміру повертає значення відстані.

Висновок: Для реалізації передачі даних по радіоканалу можна використовувати вже готові протоколи передачі даних, а також передача даних на вільній частоті, наприклад 433МГц. Такий метод дозволяє моментально з'єднувати приймач з передавачем, також не потребує автентифікації. Невід'ємним плюсом є те, що можна обрати довільне шифрування (якщо необхідне), а також надає можливість транслювати дані на декілька приймачів одночасно.

Плугова О.Б. (ВІТІ ім. Героїв Крут)
Атаманенко М.В. (ВІТІ ім. Героїв Крут)
Бригадир С.П. (ВІТІ ім. Героїв Крут)
Деркач Т.М. (ВІТІ ім. Героїв Крут)

ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ЗАСТОСУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ

Управління частинами та підрозділами, в сучасних умовах ведення бойових дій є таким же вирішальним фактором успіху, як кількість і якість військ та зброї. Співвідношення можливостей управління сторін є не менш важливим показником, чим співвідношення бойових сил та засобів.

Тому оцінка сил та засобів в сучасному бою повинна обов'язково доповнюватись оцінкою співвідношенням якості управління.

Система управління яка відповідає сучасним вимогам ведення бойових дій, здатна в значній мірі підвищити бойові можливості військового підрозділу. Відповідно збільшуються вимоги до зв'язку щодо своєчасності, достовірності, та скритності.

Саме тому виникає необхідність в забезпеченні інформаційної переваги над противником, що досягається шляхом впровадження нових способів організації зв'язку та засобів зв'язку з використанням телекомунікаційних аероплатформ, що є актуальним науково-практичним завданням, що дозволить впровадити нові способи та засоби організації радіозв'язку.

Застосування телекомунікаційних аероплатформ для організації радіозв'язку дозволить підвищити стійкість, пропускну спроможність, доступність та забезпечить більшу завадостійкість, живучість мережі зв'язку в інтересах управління військами тактичної та оперативної ланок управління.

Створення телекомунікаційних аероплатформ дозволить:

1. Розширяти територію виконання бойового завдання за рахунок передачі даних через проміжні повітряні вузли та забезпечуєть зв'язність між географічно розділеними угрупуваннями військ (зонами мобільної компоненти).

2. Підвищить стійкість системи зв'язку за рахунок створення альтернативних незалежних маршрутів обміну інформацією.

3. Збільшити зони радіопокриття за рахунок ієрархічної просторової організації мереж зв'язку з застосуванням телекомунікаційних аероплатформ різних рівнів, що виконують роль ретрансляторів, поєднуючи між собою віддалених кореспондентів.

4. Підвищити ефективность управління мережами зв'язку мобільного компоненту за рахунок скорочення довжин маршрутів обміну інформацією.

5. Підвищити тривалість функціонування мережі шляхом поетапної заміни телекомунікаційних аероплатформ.

6. Підвищити живучість системи зв'язку шляхом автоматичної реконфігурації її топології при порушенні вузлової зв'язності наземної компоненти системи.

Таким чином, застосування телекомунікаційних аероплатформ при організації і забезпеченні зв'язку в тактичній ланці управління дозволить:

організовувати зв'язок на відстані, які значно перевищують зв'язок земної хвилі в умовах прямої видимості;

дозволить значною мірою виключити фактор впливу характеру земної поверхні на дальність і стійкість зв'язку в УКХ діапазоні;

збільшити мобільність системи зв'язку;

забезпечити управління частинами і підрозділами з урахуванням умов обстановки, що склалася виходячи з завдань що виконують військами;

забезпечити стійкість та живучість функціонування системи зв'язку.

к.т.н. Погребняк Л.М. (ВІТІ ім. Героїв Крут)
Пінаєва Н.А. (ВІТІ ім. Героїв Крут)

СУЧАСНІ АУДІОКОДЕКИ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Аудіокодеки використовуються для ефективного стиснення звуку з метою зменшення вимог до сховища або пропускної здатності мережі. Робота аудіокодека має бути прозорою для кінцевого користувача (декодований звук не повинен відрізнятися від оригіналу за сприйняттям, а процес кодування/декодування не мав затримок).

За останні кілька років були розроблені різні аудіокодеки, найбільш відомими з них є Opus та EVS (англ. Enhanced Voice Services – розширені голосові послуги). Opus – це універсальний аудіокодек, який знайшов широке використання в різних додатках (платформи відеоконференцзв'язку, наприклад Google Meet, потокові сервіси, наприклад YouTube). Opus підтримує бітрейти від 6 кбіт/с до 510 кбіт/с, частоти дискретизації від 8 до 48 кГц, а також постійну та змінну швидкості передачі даних. EVS − кодек, розроблений організацією зі стандартизації 3GPP для мобільної телефонії. Як і Opus, це універсальний кодек, який працює на кількох бітрейтах (від 5,9 кбіт/с до 128 кбіт/с). Якість відновленого звуку з використанням будь-якого з цих кодеків висока при середніх і низьких бітрейтах (12-20 кбіт/с), але різко погіршується при роботі з дуже низькими бітрейтами (± 3 кбіт/с).

Аналіз науково-технічної літератури показав, що для підвищення якості обробки звуку аудіокодеками доцільно використовувати машинне навчання.

Розглянемо аудіокодек SoundStream (Google), який розширює можливості аудіокодека Lyra (побудований на основі використання нейромережі для обробки мови з низьким бітрейтом). SoundStream здатний кодувати різні типи звуку, включаючи чисту, зашумлену та реверберуючу мову, музику та звуки навколишнього середовища.

Основним технічним компонентом SoundStream є нейромережа, що складається з кодера, декодера та квантувача, які проходять наскрізне навчання. SoundStream використовує рішення в галузі нейронного аудіосинтезу для передачі звуку з високою якістю сприйняття користувачем на основі навчання дискримінатора, який обчислює комбінацію функцій змагальних та відновлювальних втрат. Після навчання кодер та декодер можна запускати на різних програмних клієнтах для ефективної передачі високоякісного звуку мережею. Під час навчання параметри кодера, квантувача та декодера оптимізуються з використанням комбінації відновлення, а також протидіючих втрат, які обчисляються дискримінатором.

Кодер SoundStream створює вектори, які можуть набувати невизначеної кількості значень. Щоб передати їх приймачеві з використанням обмеженої кількості бітів, необхідно замінити їх близькими векторами з кінцевого набору (кодової книги) у ході процесу, який відомий як векторне квантування. У SoundStream впровадили новий залишковий векторний квантувач, що складається з кількох рівнів (до 80). Такий підхід добре працює при бітрейтах близько 1 кбіт/с або нижче, але швидко досягає своїх меж при використанні вищих бітрейтів. Наприклад, навіть при швидкості передачі всього 3 кбіт/с та припущенні, що кодер видає 100 векторів в секунду, потрібно зберігати кодову книгу з більш ніж 1 мільярдом векторів, що на практиці неможливо. Оскільки при передачі звуку умови функціонування мережі можуть змінюватися, тому в ідеалі кодер має бути "масштабованим". Для цього в SoundStream впровадили метод "випадання квантувача". Під час навчання випадково відкидають кілька рівнів квантування, щоб імітувати зміну швидкості передачі даних. Це змушує декодер працювати за будь-якої швидкості передачі вхідного аудіопотоку.

Отже, сучасні аудіокодеки широко використовують методи машинного навчання для досягнення максимальної якості передачі мови при використанні низькошвидкісних каналів зв'язку. Основними напрямками подальшого розвитку аудіокодеков є перехід на нову архітектуру нейронної мережі, підтримка додаткових програмних платформ, розширення можливостей управління бітрейтом, підвищення продуктивності та досягнення вищої якості звуку.

к.т.н. Погребняк Л.М. (ВІТІ ім. Героїв Крут)
Цвіркун Т.В. (ВІТІ ім. Героїв Крут)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖЕВИХ ПРОТОКОЛІВ МАРШРУТИЗАТОРІВ MIKROTIK

Потужні професійні маршрутизатори Mikrotik характеризується широкою функціональністю, стабільністю роботи та доступністю для користувачів. Маршрутизатори Mikrotik здійснюють стабільне управління масштабними мережами та забезпечують високу швидкість передачі інформації в них при відносно низькій собівартості порівняно з аналогами інших виробників.

Завдяки широким можливостям маршрутизатори Mikrotik є основними пристроями створення безпроводових систем передачі інформації.

Окрім підтримки протоколів стандартів IEEE 802.11 маршрутизатори Mikrotik використовують пропрієтарні протоколи Nstream та NV2, що дозволяють застосовувати їх для організації зв'язку в Збройних Силах України. Мета створення цих протоколів – підвищення якості передачі інформації, пропускної здатності і дальності безпроводових з'єднань типу "точка-точка" та "точка-багатоточок".

Основними особливостями протоколу Nstream є: опитування базової станції клієнтом (polling); низькі накладні витрати на аналіз і формування заголовку пакета, що дозволяє підвищити швидкість передачі даних; відсутні обмеження щодо дальності та швидкості передачі даних, а також залежності швидкості від дальності з'єднання за рахунок використання динамічного підстроювання протоколу, залежно від типу даних, що передаються і наявних ресурсів. Протокол Nstreme здатний працювати у трьох режимах: "точка-точка" – по одному радіо модулю зі сторони передавача та приймача; "подвійна точка-точка" або Nstream2 – по два радіо модулі з кожної сторони, що підвищує пропускну здатність радіоканалу майже в 2 рази; "точка-багатоточок" – базова станція та кілька користувачів, де застосовується технологія опитування (polling), яка схожа на технологію TokenRing, що використовує спеціальний трибайтовий маркерний кадр, який переміщається по кільцю і надає власнику право передачі інформації.

Протокол NV2 (Nstream V2) на відміну від Nstream використовує TDMA (англ. Time Division Multiple Access – множинний доступ з часовим розподілом), який дозволяє отримувати доступ до одного радіочастотного каналу, виділяючи рівномірні тайм-слоти, і динамічно розподіляючи їх між користувачами враховуючи їх вимоги до смуги пропускання. Протокол NV2 підтримує QoS (англ. Quality of service – якість обслуговування) основану на вбудованих правилах і чергах, у тому числі враховується політика Firewall (англ. Firewall – вогняна стіна), пріоритети VLAN (Enhanced Voice Services і протокол MPLS (англ. Multiprotocol Label Switching – багато протокольна комутація за мітками). Крім того, протокол NV2 має власну вбудовану систему мережевої безпеки, що базується на апаратному шифруванні (протокол блокового шифрування AES-CCM з 128 біт ключем).

Отже, при встановлені з'єднання за топологією "точка-точка" на значну відстань доцільно використовувати мережевий протокол Nstreme, в якому практично зняті обмеження на дальність радіоканалу та швидкість передачі інформації в ньому. Це досить актуально при організації лінії прив'язки з використанням Р-402. У випадку встановлення з'єднання за топологією "точка-багатоточок" доцільно застосувати протокол NV2 з технологією TDMA, який на відміну від технології CSMA (англ. Carrier Sense Multiple Access with Collision Detection – множинний доступ з контролем несучої та виявленням колізій), що використовується у багатьох протоколів IEEE 802.11 для побудови такого типу з'єднань, забезпечує значну перевагу у пропускній здатності радіоканалу та швидкості доступу.

Погребняк С.В. (ВІТІ ім. Героїв Крут)

ФІЗИКО-ХІМІЧНІ ПРОЦЕСИ СТАРІННЯ ТА ЇХ ВПЛИВ НА ДІАГНОСТИЧНІ ПАРАМЕТРИ НИЗЬКОНАДІЙНИХ РАДІОЕЛЕКТРОННИХ КОМПОНЕНТІВ

Причинами відмов сучасного телекомунікаційного обладнання (ТЛКО) є наступні фактори: виробничі дефекти радіоелектронних компонентів (РЕК), довготривалі граничні, або миттєві критичні навантаження (експлуатація в стресових умовах при яких РЕК піддаються впливу підвищеним значенням температур, напруг, струму, і т.д.) та процеси природнього старіння.

З наукової точки зору найбільш складним є опис та моделювання саме процесів старіння радіоелектронних компонентів.

При вивченні зазначеної проблематики слід виходити з системного підходу та розглядати теплофізичні, фізико-хімічні й механічні властивості матеріалів, враховувати їхній взаємний вплив на властивості об'єкту контролю. Особливу увагу приділяють параметрам матеріалів та їх складових компонентів, що характеризують їхню стійкість до впливу високих і низьких температур, механічних навантажень, хімічної стабільності, електрочутливості, вологостійкості, і т.д., тому що саме вони визначають можливість використання РЕК для різних умов експлуатації, в тому числі і в польових умовах в складі зразків ТЛКО військового призначення.

Проведений аналіз показав, що типовим низьконадійним РЕК є електролітичні конденсатори які є невід'ємною частиною всіх блоків і схем сучасного ТЛКО.

Типова структура даного РЕК це металевий анод, катод та рідкій або гелевий електроліт, який діє як діелектрик. Процеси старіння саме цих компонентів призводить до зміни головних параметрів електролітичних конденсаторів (ємність та еквівалентний послідовний опір (ESR)).

Логічно стверджувати, що зміни характеристик електролітів та діелектриків пов'язані зі змінами їх фізико-хімічних властивостей. Ці зміни викликані найчастіше двома факторами: температурним – відповідно до закону Арреніуса згідно із яким швидкість протікання хімічної реакції залежить від температури. Та фактором прикладеної робочої напруги згідно із законом Лайдлера-Ейрінга відповідно до якого хімічні реакції залежать від поляризації. Отже вважаємо, що зміни властивостей (основних характеристик) РЕК викликані саме фізико-хімічними процесами під впливом температури та прикладеної робочої напруги.

В конденсаторах використовують або діелектрики з підвищеною відносною діелектричною проникністю (в основному титанатну або танталову кераміку), або полімерні діелектрики, з яких можна виготовляти тонкі плівки з великою площею поверхні. Для термостабільних герметизованих еталонних конденсаторів невеликої ємності як діелектрик використовують вакуум чи азот, відносна діелектрична проникність яких не залежить або дуже слабо залежить від температури. Однак сучасний розвиток мікроелектроніки спричинив масовий попит на дешеві РЕК в яких використовуються матеріали зі значно нижчими характеристиками ніж еталонні такі як оксиди алюмінію Al_2O_3.

Заряд на електродах конденсатора визначається виразом:

$$Q = q_0 + q_d = CU,$$

де q_0 – заряд конденсатора при умові, що його обкладки розділяє вакуум;

q_d – заряд, що зумовлений поляризацією діелектрика;

C – ємність конденсатора.

U – прикладена напруга.

Звідси випливає, що поляризація діелектрика супроводжується збільшенням ємності конденсаторів та діелектричних конструкцій C по відношенню до ємності вакуумних конденсаторів та конструкцій відповідної конфігурації C_0 в ε_r разів:

$$\frac{C}{C_0} = \frac{Q}{Q_0} = \frac{Q_0 - Q_d}{Q_0} = 1 + \frac{Q_d}{Q_0} = 1 + \frac{C_d}{C_0} = 1 + \lambda = \varepsilon_r,$$

де C_d – ємність, що зумовлена тільки поляризацією діелектрика;

ε_r – відносна діелектрична проникність.

Поляризаційний струм є основним при заряді конденсаторів. Він змінюється (спадає) за експоненціальним законом. При змінній напрузі на конденсаторі, поляризаційний струм протікає неперервно, бо не встигає повністю затухати, якщо період струму T менший постійної часу затухання. Оксиди алюмінію Al_2O_3, за рахунок своєї товщини та значній площі, яка досягається високими показниками неоднорідностей поверхні, майже не зазнають впливу поляризації і здатні до самовідновлення структури і товщини під впливом робочих значень напруги. Отже, процес природнього старіння діелектрика не залежатиме від прикладеної напруги якщо її значення буде знаходитись в межах граничних значень.

Термічний вплив на діелектрик Al_2O_3 вивчений достатньо повно та всебічно. В довідковій літературі наводяться табличні значення основних характеристик таких як щільність, коефіцієнт лінійного теплового розширення, питома (масова) теплоємність, теплопровідність. Проаналізувавши ці дані у відповідності до різної температури можна зробити висновок, що зі зростанням температури значення таких параметрів Al_2O_3 як коефіцієнт лінійного теплового розширення і питома теплоємність оксиду алюмінію зростають, а щільність і теплопровідність знижуються. При чому суттєві зміни відбуваються на температурах понад 300 °С, що не входить до робочого діапазону температур електролітичного конденсатора. Отже термічний вплив на діелектрик можна вважати несуттєвим.

На відміну від діелектрика, на електроліт в електролітичному конденсаторі, значною мірою впливають і температури навколишнього середовища і значення робочої напруги. Як відмічалося раніше, температурний вплив на електроліти призводить до їх поступового висихання внаслідок неповної герметизації корпусу, та як результат погіршення фізико-хімічних властивостей, що в свою чергу призводить до зменшення ємності конденсатора та підвищення значення його ESR.

Достатньо повно вивчене термічне старіння целюлозних матеріалів. Встановлено, що основним процесом є молекулярна деструкція. При якій виділяються гази H_2O, CO_2 і CO у пропорції 10:2:1. Інтенсивне розкладання починається при температурах 140–150 °С. Наявність кисню трохи прискорює старіння, але тільки на початковому етапі. У просоченій паперовій ізоляції (яка найчастіше використовується в алюмінієвих електролітичних кондесаторах) іонна електропровідність обумовлена дисоційованою вологою, або іншими дисоційованими домішками, що є результатом не досконалої технології виготовлення електролітичних сумішей. Звичайно електрохімічне старіння просоченої ізоляції стає помітним при температурах вище 50 °С. Саме ця температура є робочою для переважної більшості електролітичних конденсаторів. З ростом напруги старіння також прискорюється. Це обумовлено тим що при підвищенні напруги електроліти здатні до закіпання навіть при відносно невеликих значеннях температур. Визначення залежностей фізико-хімічних властивостей електролітів під впливом формфакторів температури та прикладеної напруги є метою подальших наукових досліджень.

Прогнозування показників скорочення терміну експлуатації низьконадійних РЕК в результаті процесів їх старіння є актуальної задачею. Для розв'язання якої створюється модель електролітичного конденсатору з врахуванням фізико-хімічних закономірностей процесів старіння складових компонентів під час експлуатації. Вирішення задачі прогнозування скорочення термінів експлуатації РЕК допоможе підвищувати надійність роботи сучасного ТЛКО в цілому та зменшити витрати ресурсів на їх діагностику та ремонт.

Отже, фактори наведені в роботі, значною мірою впливають на процеси старіння електролітичних конденсаторів як наймасовішого низьконадійного радіоелектронного компоненту, що в свою чергу призводить до зміни значень його основних параметрів.

Поляк І.Є. (ВІТІ ім. Героїв Крут)

ВАРІАНТ ПОБУДОВИ СИСТЕМИ СТАБІЛІЗАЦІЇ УНІФІКОВАНОЇ ПЛАТФОРМИ ТРАНСПОРТНОГО ЗАСОБУ

Необхідність використання нетипових вогневих засобів на високомобільній транспортній базі обумовлена з одного боку наявністю в достатній кількості вогневих засобів авіаційного типу (реактивних систем непритаманних сухопутним військам) з іншого обмеженим часом перебування на відкритих (стаціонарних) вогневих позиціях.

Ефективність таких систем доведено під час ведення бойових дій на близькому сході але максимальноїефективності такі системи досягатимуть у випадку використання автоматизованих пристроїв наведення та компенсації ефекту віддачі під час ведення вогню.

Сучасний стан,в з якому опинилися ЗСУ в умовах ведення бойових дій спонукає до процесу удосконалення та модернізації військової техніки, пристосуваннянетипових засобів ураження до мобільної транспортної бази наземного типу. При застосуванні сучасних зразків техніки, які адаптовані для роботи в умовах швидкої зміни обстановки, основна увага приділяється максимальному спрощенню їх налаштування, ефективному використанню особовим складом з різнім рівням технічної підготовки.

Нетипові вогневі засоби мають надзвичайно широкий спектр можливостей враження супротивника, він може використовуватися в усіх військових ланах, саме тому проблема розвитку та модернізації даних засобів є актуальною. Запропоновано спосіб побудови системи стабілізації уніфікованої платформи розташованої на транспортному засобі для нетипового озброєння на основі синтезованої системи автоматичного управління (САУ).

Ефективністьвикористання вогневих засобівоцінюється за показником купчасті влучення тазабезпечується шляхом додавання механічної системи компенсації віддачі. Для цього в контурі управління уніфікованої платформи стабілізації формується компенсаційний вплив розрахований з урахуванням коливальних властивостей транспортного засобу (характеристик підвіски, амортизаторів), точки розташування вогневого засобу відносно центру мас, кута ведення вогню в вертикальній та горизонтальній площинах, типу вогневого засобу.

Автоматична система уніфікованої платформи забезпечує оптимальні умови (недвижне розташування вогневого засобу) ведення вогню.

Частина інформації для визначення величини компенсаційного впливу формується при встановленні уніфікованої платформи на транспортний засіб. Корегування інформації відбувається автоматично після першого пострілу.

Застосування САУ забезпечує також оптимальний темп ведення вогню з врахуванням частоти власних калювань транспортного засобу.

Коливання центру мас ТЗ характеризується періодом (частотою), амплітудою й прискоренням. Наявність коливального процесу дозволяє використовувати для його аналізу та моделювання відомий математичний апарат (перетворення фур'є, та лапласа).

У зв'язку з відсутністю у ЗСУ типових мобільних систем вогневого враження та з наявністю в достатній кількості авіаційних та інших не типових систем гостро постає питання створення уніфікованої, під різну транспортну базу, стабілізованої платформи для розміщення на ній нетипових артилерійських систем.

Запропонована платформа керуватиметься автоматичною системою. Це значно спростить процес наведення та прицілювання. Окрім того, автоматичне компенсування зовнішніх впливів забезпечить більшу ймовірність влучання.

Запропонована структура багатоконтурної замкнутої САУ містить в собі ланки (передаточні функції) які розраховані з використанням пакету прикладних програм Mathcadта MatLabз метою отримання необхідних характеристик системи (синтез САУ)

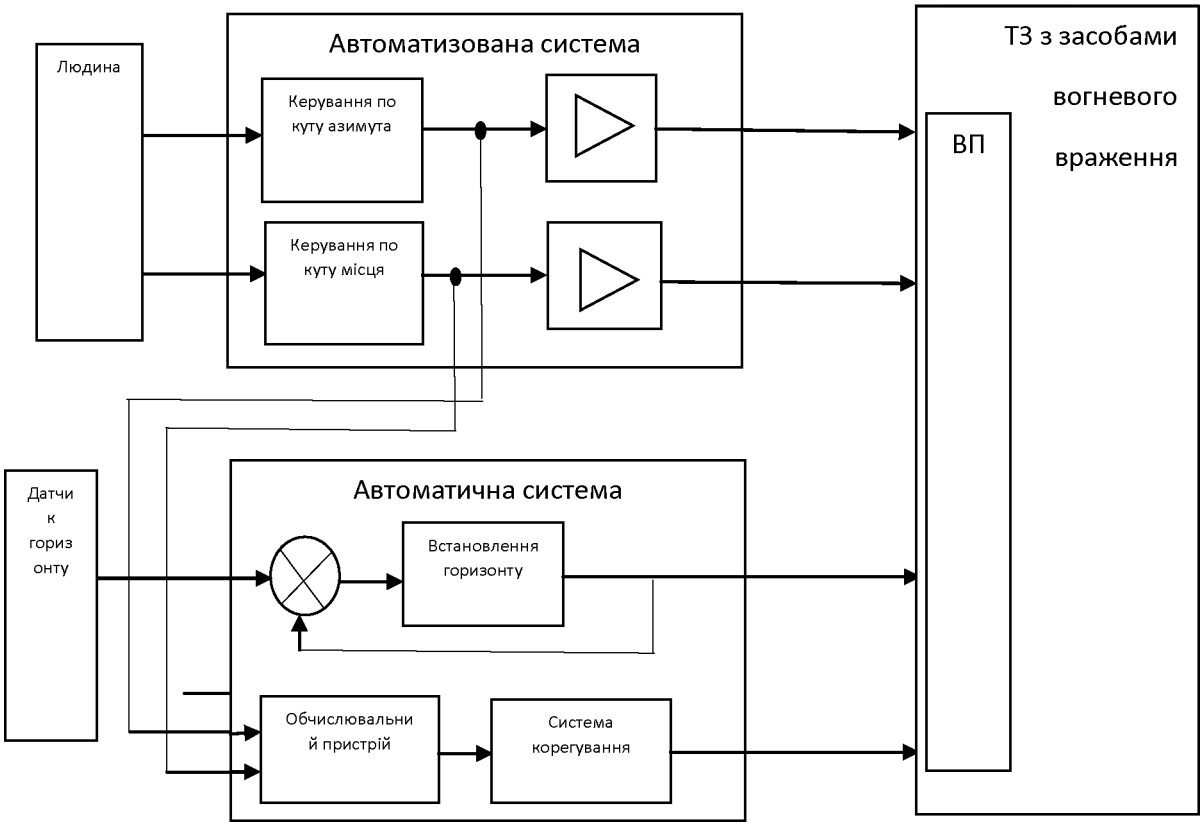


Рис.1 Функціональна схема системи керування платформи з засобом вогневого ураження

На рисунку 1 представлено складові частини запропонованої системи керування уніфікованою платформою з нетиповими вогневими засобами.

Як відмічалося, система автоматизації складається з двох основних каналів (канал автоматизованого управління та канал автоматичного керування). Завдання автоматизованої складової забезпечити дистанційне керування системою наведення перед початком ведення вогню.

Завдання автоматичної складової: забезпечити горизонтування вогневого засобу на будь якій місцевості після зупинки транспортного засобу та сформувати компенсаційний вплив на відкат при веденні вогню з урахуванням типу вогневого засобу, коливальних властивостей транспортного засобу, кута міста та кута за азимутом відносно продольної вісі транспортного засобу.

Завдання обліку наведених даних покладено на обчислювальний пристрій в канале автоматичного керування. Робота пристрою ґрунтується на розробленій в дисертаційній роботі моделі коливальних властивостей транспортного засобу.

На рисунку позначено:

- людина;
- автоматизована система яка складається з двох блоків керування (по куту азимуту та по куту місця) та двох підсилювачів після них;
- датчик горизонту;
- автоматична система яка складається з системи встановлення горизонту з зворотнім зв'язком, обчислювального пристрою та системи корегування;
- виконавчий пристрій розташований на ТЗ з засобом вогневого ураження.

Пономарьов О.А. (ВІТІ ім. Героїв Крут)
Пивоварчук С.А (ВІТІ ім. Героїв Крут)
д.п.н., к.т.н. Козубцов І.М. (ВІТІ ім. Героїв Крут)

ПРО ЗАСТОСУВАННЯ КОМП'ЮТЕРНОЇ ГРИ «СТАТИ НАЧАЛЬНИКОМ ПОЛЬОВОГО ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО ВУЗЛА» У ХОДІ ВИВЧЕННЯ ТАКТИКО-СПЕЦІАЛЬНИХ ДИСЦИПЛІН

Постановка завдання. Створення навчальних комп'ютерних ігор являє собою один з важливих напрямків у комп'ютеризації навчання [1]. З'єднання емоційної привабливості, яка притаманна грі та аудіовізуальних, обчислювальних, інформаційних та інших можливостей обчислювальної техніки несе в собі великий дидактичний (навчальний) потенціал, який може і повинен бути реалізований у військовій освіті. Сучасні заклади вищої освіти (ЗВО) і передові іноземні військові вищі навчальні (ВВНЗ) заклади активно застосовують на заняття ігрові процеси й самі комп'ютерні ігри.

Аналіз досліджень та публікацій. В роботі [2] обґрунтовують потребу в модернізації та створенні тренажно-моделювальних комплексів військового призначення для вирішення проблеми підготовки військових фахівців у ВВНЗ. Запропонована ідея гейміфікації системи військової освіти шляхом впровадження комп'ютерних ігор не є новою. В апробації [3] подана концепція самостійного навчання курсантів Сухопутних військ на навчально-тренувальних засобах методом гри на віртуальному комп'ютері. Не зважаючи на наявні напрацювання вбачається за актуальним в розробці комп'ютерної гри набуття курсантами квазі-практичного досвіду у ході вивчення тактико-спеціальних дисциплін.

Мета доповіді. Апробувати потребу в розробці та застосування комп'ютерної гри «стати начальником польового вузла зв'язку» у ході вивчення тактико-спеціальних дисциплін.

Результат дослідження. Сьогодні активно використовуються симулятори, візуалізатори і різного роду тестування, які грубо направлені на навчання, мають строгі рамки, чітко поставлені навчальні цілі. Введення відеоігор активно спостерігається в ЗВО, так як немає яскраво вираженого навчального процесу підготовки. Дітей легше залучити до ігрової платформи для розваги, в якій є сегмент навчання простим логічним, побутовим та іншим сфери життєдіяльності людини. Для введення ігор у навчальний процес ВВНЗ слід створити блоки розважальний, і навчальний, продумати сюжет і структуру обмежень дії учасника гри.

Пропонується курсантам ВВНЗ в контексті практичних занять з програмування розробити комп'ютерну навчальну гру «Стати начальником польового інформаційно-комунікаційного вузла» (СНПІКВ) в цілях підвищення освітнього процесу та використання в ході вивчення тактико-спеціальних дисциплін. Вивчення організації побудови та функціонування польових вузлів зв'язку є одним з найбільш складних питань в ході вивчення тактико-спеціальних дисциплін, при цьому гра повинна полегшити процес засвоєння і сприйняття такого складного матеріалу.

В роботі [4] при створенні гри був складений алгоритм гри і план її розробки. Були визначені завдання, основними з них були: дослідити вплив гри при вивченні теоретичного матеріалу, на що буде спрямована комп'ютерна гра – підвищення якості навчання, за рахунок мимовільного уваги, впливу на когнітивну складову мозку учня. У грі має бути реалізовано багато умов при яких гравець отримує необхідні рівень знань разом з розважальною частиною. Сюжетну лінію слід продумати таким чином, щоб фокусувати і заманювати учасника гри (курсанта) на події, що відбуваються, забезпечуючи занурення в атмосферу гри. Навчальна гра «СНПІКВ» має бути розроблена на основі поєднання структурно-логічних схем освоєння дисципліни з алгоритмом функціонування процесів ігри в середовищі комп'ютерної реальності.

Для створення гри рекомендуються програми як Unity, Visual Studio, Blender 3D. Їх вивчення показало, що вони найбільш підходять для реалізації відеоігри.

При розробці алгоритму навчальної гри «СНПІКВ» слід чітко визначені межі розважального сегменту, сформувати ясні навчальні цілі, відпрацювати деталізовану графіку і анімацію. Визначити систему заохочення та отримання ігрового досвіду. В грі має використовуватися система нарахування балів, яка на пряму залежить від ігрового військового звання учасника, у ній реалізований процес ієрархій і пріоритетів.

Наступним етапом розробки має бути проектування макетів та моделей (апаратних зв'язку, персонажів, будівель, анімованих об'єктів). Даний етап у розробці займає значно більше часу, важлива деталізація об'єктів, промальовування характерних рис персонажів і природних контурів місцевості.

Нанесення окремих деталей на макет-прототип польового ІКВ гри має значну відмінність від симуляторів і візуалізаторів, тим, що вони розташовуються в складі цілого польового вузла зв'язку і мають свою структуру. Розміщення апаратних зв'язку проводилося згідно основних керівних документів Збройних Сил України.

В середовищі Visual Studio, можна описати фізику гри, закономірність руху кулі, автомобіля і т. п., розкрити взаємодію ігрових об'єктів на макеті польового ІКВ, оживляє дії предмета на карті місцевості (хмари, вода, вітер, рух сонця, тінь об'єктів). Це етап у розробці займає не мало важливу роль, адже без використання коду не буде ефекту заглибленості в плановану обстановку і ігрову реальність.

Перед початком гри користувачеві необхідно зареєструватися, ввести прізвище та ім'я, логін і пароль. Після цього гравцеві пропонується вибрати режим гри, це режими вузол зв'язку командного пункту, який знаходиться в розробці. Вибравши вузол зв'язку командного пункту певного рівня, гравець опиняється на віртуальній майданчику, де отримує завдання на проходження завдання. Отримавши завдання, гравець відправляється до вузла зв'язку, рухаючись за вказівниками. Починає вивчення з структури. Далі гравцеві надається можливість почати вивчення тактико-технічних характеристик (ТТХ), складу та призначення апаратних зв'язку. Для закріплення отриманих знань і отримання «досвіду» гравець може пройти тестування, яке визначить рівень його підготовки «досвіду» і надасть відповідне військове звання за успішне проходження елемента. Покинувши зону вивчення групи каналоутворення вже в новому військовому званні (по грі «сержант») у випадковому порядку і будь-якій галузі можуть випадати кейси з додатковими завданнями «бонусами» такими як, стрільба зі стрілецької зброї, виконання прийому і передачі радіограм кодом Морзе, виконання нормативів з РХБЗ підготовки, знань положення статей статутів ЗС України.

Висновки. Таким чином, впровадження гри позитивно може впливати на засвоєння навчального матеріалу тактико-спеціальних дисциплін. Запроваджуючи такий тип навчання в освітній процес, можна активізувати пізнавальний процес, спростити саму програму навчання, направивши виграний час на ті теми або дисципліни, які теж вимагають достатнього розуміння курсантів. При вивченні курсант повинен знати структури польових вузлів зв'язку, порядок функціонування їх елементів, організацію взаємодії з підлеглими або ж вищого рівня вузлами зв'язку. Занурюючись у віртуальну ігрову атмосферу, учасник навчальної гри «СНПІКВ» не тільки вивчає знання техніки зв'язку, але і набуває знань оперативно-технічної служби та інших питань, досліджуваних у ході бойової підготовки військовослужбовців

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jane McGonigal. Reality is broken: why games make us better and how they can change the world. New York: Penguin Books, 2011. 402 p.

2. Руснак І.С., Шевченко В.Л. Проблеми модернізації та створення тренажно-моделювальних комплексів військового призначення. Наука і оборона. 2002. №1. С. 32-39.

3. Козубцов І.М. Концепція самостійного навчання курсантів Сухопутних військ на навчально-тренувальних засобах методом гри на віртуальному комп'ютері. «Перспективи розвитку озброєння і військової техніки Сухопутних військ». Друга всеукраїнська науково-технічна конференція (Львів, 28-29 квітня 2009 р.). С. 77.

4. Katie Salen and Eric Zimmerman. Rules of Play – Game Design Fundamentals. MIT Press, 2004. 670 p.

к.т.н. Прокопенко Є.В. (НАДПСУ)
к.т.н. Мул Д.А. (НАДПСУ)
Равлюк В.В. (НАДПСУ)

ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИКОРДОННОГО ВІДОМСТВА В УМОВАХ ВОЄННОГО СТАНУ

Актуальність. В умовах безпрецедентної збройної агресії Російської Федерації проти України, бойові дії ведуться не тільки із застосування людських ресурсів, вогнепальної зброї, артилерії, літаків, танків тощо на полях бою, та не менш значущою ареною боротьби є інформаційний простір.

Постановка задачі. Держава-агресор володіє розвинутими засобами та технологіями масових комунікацій та уміло застосовує їх на свою користь при ведені інформаційної війни. Процес виробництва та поширення завідомо недостовірної інформації з метою внести у свідому та осмислену діяльність людини руйнівні ідеї та подальшого її повного контролю і маніпулювання її поведінкою, є пріоритетним напрямком ведення інформаційної війни нашим агресором. Перемога ворога у цій війні призведе до того, що українське суспільство буде інфіковане проросійською ідеологією та стане приреченим до повного та цілковитого програшу державі-окупанту.

Отже, проблеми забезпечення інформаційної безпеки держави, як невід'ємної складової національної безпеки, для нашої країни є вельми актуальними, які тісно пов'язані з принципом забезпечення недоторканості державного кордону України.

Основні положення. Під національною безпекою, відповідно до Закону України «Про національну безпеку України», розуміють захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, визначено «Стратегією інформаційної безпеки» яка затверджена Указом Президента України від 28 грудня 2021 року № 685/2021 також Законом України «Про національну безпеку України» передбачено забезпечення інформаційної безпеки держави одним з пріоритетних напрямків державної політики у сферах національної безпеки і оборони України поряд із політичною, військовою, економічною, соціальною та екологічною безпекою.

Необхідність розмежування інформаційної безпеки за геополітичними рівнями покликана в першу чергу активізацією міжнародних терористичних, екстремістських організацій та злочинних угруповань, окремих держав, які здійснюють інформаційні впливи на громадян, суспільство, держави з метою реалізації своїх інтересів. Тому забезпечення інформаційної безпеки на міжнародному, регіональному та національному рівнях є однією з найважливіших складових системи забезпечення національної безпеки для будь-якої держави.

Інформаційна безпека, як складова національної безпеки – стан захищеності життєво важливих інтересів людини, суспільства і держави, коли виключається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Міжнародна безпека – це система міжнародних відносин щодо дотримання всіма державами загальновизнаних принципів і норм міжнародного права та загальнолюдських інтересів.

На міжнародному рівні інформаційна безпека є транснаціональною задачею. Вона не може забезпечуватися однією державою. Це задача усіх цивілізованих країн. Тільки сумісні зусилля з питань забезпечення інформаційної безпеки матимуть позитивний ефект та

сприятимуть підвищенню рівня міжнародної безпеки в інформаційній сфері, як окремо взятої держави, так і світового співтовариства в цілому.

Міжнародна інформаційна безпека формується на основі національної та регіональної інформаційної безпеки.

Регіональна безпека є похідною від національної і міжнародної безпеки та включає наступні види безпеки: політичну, економічну, екологічну, інформаційну, кібернетичну та інші види безпеки.

Інформаційна безпека окремо взятого регіону не може бути в достатній мірі забезпечена поза рамками систем інформаційної безпеки більш високого рівня. Але слід відмітити, що саме на регіональному рівні закладаються фундаментальні основи інформаційної безпеки міждержавних утворень, націй і народів, їх стійкого та стабільного розвитку.

Сучасний підхід до вирішення питань інформаційної безпеки на національному рівні є те, що вони вирішуються не суто індивідуально, а спільними зусиллями низки держав. При цьому їх інтереси, як геополітичного, так і геостратегічного рівнів, як правило, збігаються, або принципово не суперечать один одному.

Пропонуємо розглядати інформаційну безпеку в діяльності Державної прикордонної служби України, як комплекс заходів, спрямованих на своєчасне реагування на виклики та унеможливлення загроз в інформаційній сфері, які можуть нести шкоди суб'єктам прикордонної сфери та прикордонної безпеки, а також забезпечення цілісності інформації, порядку доступу до неї. З урахуванням вище наведеного можна стверджувати що захист інформації є складовою частиною інформаційної безпеки.

Не зважаючи на окремі обмеження правового режиму воєнного стану в Україні, наявності викликів та загроз інформаційної безпеки в кіберпросторі, інформаційні ресурси критичної інфраструктури мають буди захищені у відповідності до керівних документів з питань захисту інформації та функціонувати в межах наявної розробленої комплексної системи захисту інформації. Вимоги, щодо захисту інформації в інформаційно-комунікаційних системах під час дії воєнного часу не змінюються, вони визначені в законодавстві України та інших нормативних документів з питань технічного захисту інформації.

Сучасна модель охорони державного кордону передбачає використання в Держприкордонслужбі єдиного інформаційного простору – сукупності баз та банків даних, технологій їх ведення та використання, інформаційних систем та телекомунікаційних мереж, що функціонують на основі єдиних принципів і по загальним правилам. Особливої гостроти проблема захисту набуває у зв'язку із масовою комп'ютеризацією інформаційних процесів, широким впровадженням інформаційно-комунікаційних мереж з доступом до їх ресурсів маси користувачів.

Висновок. Забезпечення інформаційної безпеки держави шляхом ефективної протидії інформаційним загрозам національним інтересам дозволяють захистити інформаційний простір і державу від інформаційних загроз. Ключова роль у забезпеченні безпеки на усіх рівнях поступово починає відводиться інформаційній безпеці.

Основним завданням, яке необхідно вирішити з організації надійного захисту інформаційних ресурсів – є проведення аналізу захищеності об'єкта захисту, що включає в себе: дослідження характеру потоків інформації, яка циркулює в об'єкті; її властивостей; можливих загроз для неї та характеру їх виникнення; оцінка структури інформаційної системи, яка слугує для накопичення, зберігання, використання та видачі інформації; визначення каналів витоку інформації в даній інформаційній системі. На основі цього аналізу можлива побудова моделі загроз та потенційно можливих сценаріїв злочинних дій порушників безпеки інформації.

к.т.н. Радзівілов Г.Д. (ВІТІ ім. Героїв Крут)

СИСТЕМИ АВТОМАТИЧНОГО УПРАВЛІННЯ З ДИНАМІЧНИМ ВИБОРОМ СТРУКТУРИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ТА НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ

Сучасний етап теорії автоматичного управління характеризується розв'язанням задач, що враховують неточність знань про об'єкти управління та діючих на них збурень, відсутністю необхідної апріорної інформації для етапу проектування систем автоматичного управління (САУ). Це стосується проектування систем автоматичного управління діаграмам направленості антен, систем стабілізації різного роду, систем управління траєкторією польоту БПЛА та ін. Традиційні методи проектування САУ багато в чому не задовольняють сучасним вимогам. По-перше, при традиційних методах проектування відсутній етап системного аналізу всієї сукупності систем управління, як єдиної системи, і внаслідок цього коригування структури системи та зв'язку між її функціональними елементами вносяться на етапі дослідно-промислових випробувань системи. По-друге, час розробки систем продовжує зростати разом із ускладненням систем. По-третє, внаслідок ускладнення систем та безперервного підвищення вимог до систем щодо точності та швидкодії практично виключається багатоваріантне проектування.

В теорії автоматичного управління є досить багато методів, які дозволяють оптимізувати роботу систем за тими чи іншими критеріями якості при різних обмеженнях. Наприклад відомо, що метод, запропонований професором Гостєвим В.І. на основі ПІД-регулятору вважається досить близьким до оптимального, який в свою чергу заснований на теорії передбачення Колмогорова-Вінера. Також професором Зайцевим Г.Ф. був запропонований метод синтезу систем автоматичного управління на основі диференційної вилки, який дав можливість проектування САУ з непрямим виміром збурюючого впливу.

Однак при зростанні вимог до якості керування динамічна точність регулювання з типовими ПІД-регуляторами та диференційними вилками в одноконтурних САУ не забезпечується. У таких випадках зазвичай йдуть на ускладнення системи. Прикладом можуть бути каскадні двоконтурні та багатоконтурні САУ. Аналіз методів проектування САУ показав, що універсальних рекомендацій щодо вибору структури системи в умовах невизначеного характеру збурюючих впливів при умові підвищення вимог до якості управління не існує. При використанні традиційних методів управління, які спираються на теорію лінійних систем стає необхідним повніший і точніший математичний опис досліджуваних процесів і об'єктів. Однак у реальних об'єктах неминуче є невизначеність (неповнота інформації), яка не враховується в їх математичних моделях, а система управління такими об'єктами не забезпечує високих показників якості і навіть може виявитися непрацездатною. З позицій системного підходу практично всі звичайні САУ мають бути віднесені до систем з неповною інформацією щодо моделі об'єкта. У зв'язку з цим виникає необхідність у розробці робастних систем управління, що дозволяють забезпечити високу якість функціонування системи в умовах, коли об'єкт управління відрізняється від розрахункової моделі або коли його математична модель невідома чи неповна.

В процесі проектування таких систем виникає відоме протиріччя між підвищенням коефіцієнту підсилення системи та її стійкістю. Усунення вказаного протиріччя можливе вибором «компромісного рішення» між підвищенням коефіцієнту підсилення та забезпеченням стійкості системи. Цей метод не завжди дає повне рішення вказаної проблеми, оскільки форма перехідного процесу системи може бути повільно затухаючою, що незмінно вплине на якість системи.

Тому в останній час знаходять місце «м'які» обчислення (soft computing), які забезпечують достатню, майже оптимальну якість управління в умовах невизначеності при

відносно невисокому рівні витрат ресурсів. Цей метод об'єднує в собі такі інтелектуальні технології, як нечітка логіка (fuzzy-logic), нейронні мережі та еволюційні алгоритми. Використання нечіткої логіки та нейронних мереж є найбільш поширеним. На думку експертів, в найближчий час біля 90% всіх САУ будуть розроблені на основі нечіткої логіки з застосуванням нейронних мереж. Це є одним з можливих шляхів підвищення якості систем автоматичного управління.

Поряд із системами управління, які побудовані на нечіткій логіці, метод нейроуправління, як самостійний розділ сучасної теорії управління, що спирається на застосування нейронних мереж активно розвивається в останні роки для вирішення завдань управління складними динамічними системами. А саме системами з невизначеностями, нестаціонарними системами, слабовідтворюваними процесами та ін., що пов'язано з розвитком високих технологій у різних галузях науки. Нейронна мережа являє собою високо паралельну динамічну нелінійну систему, конфігурація якої може автоматично змінюватися в залежності від системи управління, завдання і параметрів зовнішнього середовища, налаштовуючись на необхідну вихідну реакцію. У разі реалізації нейроуправління стає непотрібним спроба опису нелінійними диференціальними рівняннями систем із змінними параметрами та спроба вирішення цих рівнянь за допомогою алгоритмів, адекватних обчислювачам з архітектурою Фон-Неймана. Це в свою чергу дає можливість вирішення проблеми проектування САУ з високим коефіцієнтом підсилення та швидко затухаючим перехідним процесом.

Радченко М.М. (ВІТІ ім. Героїв Крут)
Титаренко А.В. (ВІТІ ім. Героїв Крут)
Скляров О.В. (ВІТІ ім. Героїв Крут)

ЕТАПИ ВПРОВАДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ В СИСТЕМУ ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Постановка завдання у загальному вигляді

На ряду із іншими важливими заходами що проводяться військово-політичним керівництвом країни щодо вдосконалення систем управління, формування оборонних ресурсів та прийняття на озброєння нових зразків озброєння та військової техніки є створення сучасної інформаційної інфраструктури складових сил оборони, в яку повинні упроваджуватись сучасні інформаційні технології, автоматизація управлінських процесів і цифровізація діяльності органів управління що відображено в завданнях Стратегій національної та воєнної безпек України.

Наведене завдання потребує здійснення цілеспрямованих, скоординованих за термінами, обсягами ресурсного забезпечення заходів щодо приведення існуючої інформаційної інфраструктури складових сил оборони до сучасних потреб тому автори вважають актуальним пошук шляхів впровадження телекомунікаційних аероплатформ (далі – ТА) в систему зв'язку (далі –СЗ) ЗС України на базі безпілотних авіаційних комплексів (далі – БпАК).

Виклад основного матеріалу

Одним із завдань, що покладається на ТА, є здійснення ретрансляції зв'язку в таких умовах де в силу географічних чи кліматичних факторів виконання завдань класичним способом зі зв'язку є неможливим або недоцільним через значні затрати ресурсів.

На сьогодні, з однієї сторони, рішення щодо створення ТА ускладнюється такими факторами як: наявністю різнорідних радіозасобів УКХ/КХ діапазонів, які могли б використовуватись в якості ТА; відсутністю довготривалих практичних досліджень використання таких радіозасобів у різноманітних умовах, високою вартістю таких досліджень. З іншої сторони, театр воєнних дій в Україні створює бойові умови застосування БпАК де можливо перевіряти їх функціонування в умовах реальної протидії з боку систем ППО і РЕБ агресора що дозволяє українським виробникам таких комплексів накопичувати унікальний досвід щодо створення нових технології виготовлення та вдосконалення існуючих.

Впровадження ТА пропонується здійснювати поетапно. Спільні риси етапів полягають у наступному:

застосування БпАК для підтримання (відновлення) збереження заданої якості зв'язку для підрозділів ЗС України;

поступовий перехід від існуючих радіозасобів до тих, які плануються на постачання, із зміною платформ БпАК, які створюються вітчизняною промисловістю;

здійснення заходів щодо внесення змін до штатів підрозділів зв'язку, де будуть розміщені БпАК-радіоретранслятори та підготовку особового складу цих підрозділів до виконання завдань за призначенням.

Кількість, черговість та зміст етапів уточнюються у ході впровадження з урахуванням змін у перспективній системі зв'язку оперативно-тактичної ланки управління ЗС України а також із ураховуванням призначених для таких цілей фінансових ресурсів.

Перший етап полягає у здійснені заходів щодо:

створення повітряного радіоретранслятора на базі БпАК для ретрансляції цифрового радіозв'язку стандарту DMR, з огляду на широке розповсюдження радіозасобів наведеного стандарту у військових підрозділах (використання ретрансляторів стандарту DMR можливе у так називаний перехідний період);

створення комплекту ретранслятора та БпАК для ретрансляції цифрового радіозв'язку утвореного радіостанціями, які використовують шумоподібний сигнал, що дозволятиме забезпечити спеціальні підрозділи захищеним радіозв'язком, в діяльності яких сам факт виходу на радіозвязок є критичним.

Другий етап – здійснити заходи щодо:

створення повітряного ретранслятора на базі БпАК для роботи в радіомережах, які утворюються радіозасобами виробництва компаній Aselsan та Harris, що дозволить забезпечити підрозділи Сухопутних військ, Десантно штурмових військ та Сил спеціальних операцій ЗС України завадостійким, захищеним радіозв'язком в рамках відповідних завдань проведення нарощування наземної та повітряної складової утвореної системи зв'язку.

Третій етап – здійснити заходи щодо:

вибору (створення) станцій широкосмугового доступу та проведення випробувань щодо постановки їх на озброєння;

проведення оснащення призначених підрозділів станціями широкосмугового доступу;

створення ТА для організації мереж широкосмугового доступу, маршрутизації та ретрансляції УКХ радіомереж в рамках поставлених завдань проведення нарощування наземної та повітряної складової утвореної системи зв'язку.

Четвертий етап – здійснити заходи щодо:

проведення досліджень щодо необхідності розробки, застосування та розвитку телекомунікаційних систем на основі висотних аероплатформ та можливостей супутникового зв'язку.

Виконання вищенаведених етапів дозволить створити повітряний ешелон системи зв'язку оперативно-тактичної ланки управління ЗС України та дозволить забезпечити:

оперативне розгортання резервної або додаткової мережі радіозв'язку з наземними абонентами, в особливих випадках здійснювати маневр зв'язком у разі відмови діючого сегмента системи зв'язку;

радіозв'язком підрозділи, що діють у територіальному відриві від основних сил оборони та у складних географічних умовах (гори, ліс, щільна міська забудова);

підвищення рівня прихованості факту радіозв'язку за рахунок зниження рівня потужності передачі радіозасобів у тих випадках де факт виявлення роботи радіозасобів є критичним.

На сьогодні, аналіз технічних характеристик БпАК, що виробляються підприємствами України, за такими параметрами як: корисне навантаження, час автономного польоту, висота польоту, стійкість до впливу РЕБ та інш. показує що вітчизняні виробники у випадку отримання ними технічного завдання на виготовлення ТА спроможні виробляти названі вироби з очікуваним рівнем якості.

При реалізації замовлення на створення дослідних зразків ТА доцільно розглянути спроможності таких виробників, як: ТОВ "Укрспецсистемс"; ТОВ науково-виробниче підприємство "Spaitech"; Науково-виробничий центр безпілотної авіації "Віраж"; Держа́вне підприємство "Антонов".

Висновки.

Запропоновані етапи впровадження телекомунікаційних аероплатформ дадуть змогу, з урахуванням фінансових ресурсів призначених для цієї мети, забезпечити нарощування транспортної мережі СЗ ЗС України шляхом доповнення повітряної складової телекомунікаційними аероплатформами.

Виконання вище наведених етапів дозволить:

забезпечити збільшення зони покриття радіозв'язку існуючої радіомережі утворених наявними радіозасобами стандарту DMR та організацію захищеного радіозв'язку утвореного радіостанціями, які використовують шумоподібний сигнал;

збільшити зону покриття завадостійкого та захищеного радіозв'язку утвореної наявними радіостанціями виробництва компаній країн-партнерів;

розгорнути на базі станцій широкосмугового зв'язку повноцінну, захищену транспортну мережу радіодоступу з можливістю швидкісної передачі даних та маршрутизації.

У цілому, все вище наведене дасть поштовх до якісно нового рівня забезпечення виконання завдань зі зв'язку через повітряну складову СЗ ЗС України.

Садаєв А.Ю. (ДНДІ ВС ОВТ)
к.т.н Аркушенко П.Л. (ДНДІ ВС ОВТ)
Кузьміч О.Є. (ДНДІ ВС ОВТ)
Гузій Є.О. (ДНДІ ВС ОВТ)

АНАЛІЗ ЗАГАЛЬНИХ ВИМОГ ДО РАДІОКАНАЛУ БЕЗПЕРЕРВНОЇ ПЕРЕДАЧІ ДАНИХ ОБ'ЄКТИВНОГО КОНТРОЛЮ

В питанні забезпечення безпеки польотів та підтриманні справного стану повітряних суден особливе місце займають бортові засоби об'єктивного контролю.

Польотна інформація реєстрована за допомогою бортового аварійно-експлуатаційного реєстратора дозволяє оцінити не тільки техніку пілотування та повноту виконання бойового завдання, та й технічний стан повітряного судна, його систем, агрегатів, і в разі авіаційної події з'ясувати причини та фактори які сприяли її виникненню.

Принцип роботи бортових засобів реєстрації параметрів польоту полягає в тому що, значення фізичних параметрів (швидкість, висота та інше) отриманих з первинних перетворювачів (датчиків об'єкта), формуються у вигляді 8-розрядного слова, яке зберігається на твердотільному накопичувачі. Ці накопичувачі мають захищений корпус та забарвлюються у яскравий помаранчевий колір, для полегшення виявлення його серед уламків літака та в деяких модифікаціях оснащується гідроакустичним маяком для пошуку його під водою.

Оскільки, внаслідок аварій, обладнання літака зазнає величезних руйнівних впливів, аварійні самописці повинні бути надійно захищені, але є ймовірність того, що накопичувач може бути пошкодженим і дані з нього доведеться відновлювати або взагалі втраченими.

Крім того, у багатьох випадках роботи з пошуку самописців проводяться із залученням великих сил та засобів не лише авіації, а й флоту та інших рятувальних підрозділів, що потребує багато часу та величезних фінансових витрат.[1] Треба відмітити, що в умовах відкритої збройної агресії російської федерації треба враховувати можливість падіння повітряного судна в наслідок бойового пошкодження, або відмови обладнання на тимчасово окупованої території, де провести пошук накопичувача польотної інформації на даний час не можливо.

Тому пропонується оцінити технічну можливість реалізації передачі в режимі реального часу даних, що записуються бортовими засобами реєстрації, на віддалені сервери диспетчерського пункту управління в режимі онлайн. У такому випадку пошуки і відновлення інформації не знадобиться, а необхідна польотна інформація буде оперативно отримана та проаналізована.

Для вирішення питання організації передачі польотної інформації з бортових реєстраторів на наземні пункти управління необхідно сформулювати вимоги до радіоканалу, який забезпечить цю передачу. [2]

Розглянемо алгоритм роботи аварійно-експлуатаційного реєстратора на прикладі реєстратора типу БУР-4-1, які останнім часом, встановлюються на переважну більшість повітряних суден державної авіації України. Реєстратор здатний реєструвати 28 аналогових параметрів і 32 бінарних сигнали. До складу реєстратора входить блок збору і перетворення інформації, отриманої з датчиків, твердотільний накопичувач та пульт управління. Датчики визначають висоту, швидкість, курс літака, положення органів керування повітряним судном та отриману фізичну величину перетворюють в електричний сигнал, який в подальшому перетворюється в цифровий сигнал та надходить на реєстрацію в твердотільний накопичувач. [3] Даний цифровий сигнал пропонується паралельно з реєстрацією надсилати на передаючий пристрій, якій буде формувати інформаційні пакети та надсилати їх на наземний пункт керування польотами. Для скорочення обсягів інформації, яка підлягає

передачі необхідно відпрацювати перелік найбільш важливих параметрів для кожного типу повітряного судна (далі ПС).

На підставі наведеного можливо сформувати основні вимоги до радіоканалу передачі даних, який повинен:

- забезпечувати стабільну швидкість передачі даних;
- бути захищеним від несанкціонованого доступу;
- забезпечувати автоматичну передачу даних без втручання екіпажу ПС;
- бути високо надійними та зі значною стійкістю до завад.
- при передачі сигналу був сформований так, щоб спотворення були мінімальними;

Технічна реалізація та впровадження даного способу передачі польотної інформації на наземний пункт управління польотами дозволить суттєво скоротити витрати часу при розслідуванні авіаційних подій та здійснювати оперативний доступ до необхідних даних у разі бойового ураження ПС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Безопасность полетов гражданских судов"/ В.В Воробьева. [Электронный ресурс].
2. Авиационные связи и системы отчетности / доктор Мартин Уит Хаг: университет Огайо США. 2009. [Электронный ресурс].
3. "Руководство по технической эксалуатации БУР-4-1" 8И1.582.017-02 РЭ

к.т.н. Самойлов І.В. (ІСЗЗІ КПІ ім. Ігоря Сікорського)
к.т.н. Конотопець М.М. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

МОДЕЛЬ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Зі зростанням складності об'єктів інформатизації, зміни множини та характеру загроз інформаційної безпеки, особливо загроз несанкціонованого віддаленого доступу до ресурсів і процесам критичних інформаційних систем, задача оцінки захищеності є актуальною.

Захищеність інформаційних систем визначається виходячи зі збитків організації, пов'язаних з реалізацією загроз, які носять імовірнісний характер. Коефіцієнти небезпеки представляються нечіткими величинами, а показники захищеності інформаційних систем визначаються за допомогою нечітких відношень між коефіцієнтом небезпеки множини загроз і ступеня захищеності інформаційної системи. В свою чергу оцінку захищеності можна побічно зв'язати з запобіганням збитків і використовувати експертні оцінки для зіставлення множини загроз з потенційними збитками від їх реалізації та розміру збитків з містом реалізації загрози в структурі інформаційної системи. Для формалізації експертної інформації при моделюванні причинно-наслідкових зв'язків зручно використовувати теорію нечітких множин. Нечітка модель будується на основі композиційного правила виведення Заде, в якому носієм інформації є матриця нечітких відношень "загрози–збитки", що зв'язує вектор мір значимості загроз і вектор мір значимості збитків.

Нехай відомо: множина вхідних змінних $X = (x_1, x_2, \ldots, x_n)$; $x_i \in [\underline{x_i}, \overline{x_i}]$, $i = \overline{1, n}$; множина вихідних змінних $Y = (y_1, y_2, \ldots, y_m)$; $y_j \in [\underline{y_j}, \overline{y_j}]$, $j = \overline{1, m}$; множина загроз $D = (d_1, d_2, \ldots, d_n)$, де загроза d_i, $i = \overline{1, n}$, інтерпретується як нечіткий терм, що описує змінну x_i; множина збитків $S = (s_1, s_2, \ldots, s_m)$, де збиток s_j, $j = \overline{1, m}$, інтерпретується як нечіткий терм, що описує змінну y_j; відношення між загрозами і збитками $R \subseteq D \times S$.

Задача оцінки захищеності може формулюватись у формі прямого і оберненого логічного виведення. При прямому логічному виведенні необхідно визначити збитки S^* для заданого вектора вхідних змінних X^*. При оберненому логічному виведенні необхідно відновити загрози D^* для заданого вектора вихідних змінних Y^*. Розв'язання останньої задачі вимагає побудови моделі на базі нечітких відношень. В загальному випадку для прийняття рішення необхідно виконати наступні дії: перетворити значення вхідних змінних в міру значимості загроз; використовуючи композиційне правило виведення Заде та матрицю нечітких відношень отримати міри значимості збитків; виконати операцію пониження типу та перетворити міри значимості збитків у значення вихідних змінних. В результаті виконання цих дій отримуємо модель оцінки захищеності інформаційних систем на базі нечітких відношень, яка оперує з невизначеністю шляхом використання інтервальних функції належності нечітких термів загроз і збитків, а також використовує функції належності I типу, які дозволяють моделювати неточність вхідних даних:

$$Y = f_R^{II}(X,\ \widetilde{R},\ C_X,\ \underline{G}_{\widetilde{D}},\ \overline{G}_{\widetilde{D}},\ C_{\widetilde{D}},\ \underline{G}_{\widetilde{S}},\ \overline{G}_{\widetilde{S}},\ C_{\widetilde{S}}),$$

де $X = (x_1, x_2, \ldots, x_n)$ – вектор вхідних змінних; $\widetilde{R} = \left\{[\underline{r_{ij}}, \overline{r_{ij}}]\right\}$ – матриця інтервальних нечітких відношень II типу; $C_X = (c_1^*, c_2^*, \ldots, c_n^*)$ – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних даних; $\underline{G}_{\widetilde{D}}, \overline{G}_{\widetilde{D}}, C_{\widetilde{D}}$ – вектори параметрів функцій належності вхідних змінних; $\underline{G}_{\widetilde{S}}, \overline{G}_{\widetilde{S}}, C_{\widetilde{S}}$ – вектори параметрів функцій належності вихідних змінних; f_R^{II} – оператор зв'язку "входи-виходи" для нечіткої системи II типу.

Таким чином на основі аналізу захищеності інформаційних систем можна прогнозувати можливий збиток від реалізації загрози, його оцінку та рекомендувати необхідні дії.

PhD Самокіш А.В. (ХНУПС)
PhD Толкаченко Є.А. (ХНУПС)
Клімочкіна А.О. (ХНУПС)
Ковінський В.І. (ХНУПС)

МОДЕЛЬ ПРОЦЕСУ ПОБУДОВИ МАРШРУТУ ГРУПИ БПЛА ДО ЦІЛЬОВОГО ОБ'ЄКТА

Актуальність. Сучасний етап розвитку безпілотних літальних апаратів (БПЛА) зумовлює їх активне використання при вирішення різноманітних складних завдань в широкому діапазоні людської діяльності. Для підвищення ефективності застосування БПЛА яку у військових так і цивільних сферах необхідним є застосування групи БПЛА. Група БПЛА дозволяє як отримувати значні тактичні переваги на полі бою, так і для вирішення завдань пошуку та порятунку в реальних умовах. Основними перевагами, застосування груп БПЛА є:

− підвищення надійності (втрата частини БПЛА не призводить до зриву цільового завдання);

− гнучкість (здатність групи БПЛА до реконфігурації);

− потенційна можливість розвитку та ускладнення вирішувальних завдань на основі включення до групи БПЛА різного цільового призначення.

Проте, практична реалізація можливостей застосування групи БПЛА ускладняються відсутністю конструктивних алгоритмів планування та управління польотом групи БПЛА. Тому актуальним є дослідження підходів планування та оптимізації управління траєкторією польоту групи БПЛА при виконанні цільового завдання.

Постановка задачі. Особливість процесів прийняття рішень при плануванні та реалізації польоту групи БПЛА полягає в тому, що вони об'єктивно повинні базуватися на даних, що отримані на основі обробки нечіткої інформації з використанням нечітких правил. Звідси випливає проблема формалізації неявно заданих причинно-наслідкових зв'язків на основі явних і неявних експертних знань про процес планування авіаційного удару у вигляді, доступному для обробки в системах управління БПЛА.

Метою роботи є підвищення обгрунтованості прийняття рішень у процесі планування та реалізації польоту групи БПЛА при виконанні цільового завдання..

Основні положення

Застосування нечіткої логіки для реалізації систем планування маршруту групи БПЛА до об'єкту цільового завдання передбачає вирішення завдань: формування нечітких наборів для подання позицій і у деяких випадках форм об'єктів, наявних в операційній зоні; планування простих нечітких поведінок; активізація необхідного нечіткої поведінки (або комбінацій поведінок) залежно від поточного стану повітряної обстановки. Поведінка групи БПЛА є множиною окремих дій, причому вибір певної поведінки залежить від стану ПО. Основна проблема при синтезі алгоритму планування маршруту, заснованого на сукупності кількох окремих поведінок, полягає у необхідності їх координації. Координація поведінки – завдання вибору певної дії з набору заданих поведінок. Пропонується наступна структура системи планування маршруту польоту групи БПЛА (рис. 1).

На керуючому рівні на основі оцінки обстановки на кожному етапі маршруту приймається рішення, яке активізує певні дії замість того, щоб обробити всі поведінки і потім їх комбінувати. Такий підхід скорочує час і витрати на обчислювальні ресурси. Рішення завдання планування маршруту до об'єкта авіаційного удару із застосуванням координації поведінок передбачає декомпозицію основної (загальної) поведінки на кілька простих окремих поведінок, кожна з яких подано сукупністю нечітких продукційних правил. Формуються такі положення: при польоті групи БПЛА до об'єкта цільового завдання застосовуються наступні поведінки: "політ до цілі", "огинання перешкоди", "політ уздовж

складок місцевості"; поведінка "режим найбільшої дальності польоту"; поведінка "режим найбільшої тривалості польоту".

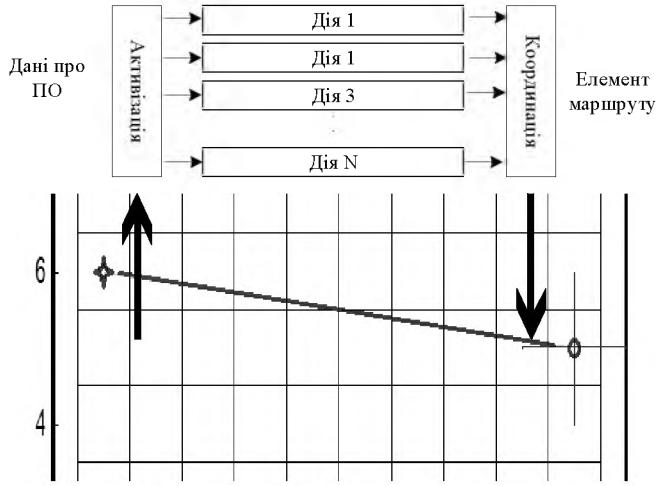


Рис. 1 – Модель процесу побудови маршруту групи БПЛА до цільового об'єкта

Кожну окрему поведінку складено з набору нечітких логічних правил, що забезпечують досить точне досягнення мети; до числа вихідних параметрів для кожного окремого поведінки відносяться: курс (heading) і швидкість (velocity); висота польоту (altitude). Координуючий рівень визначає пріоритет виконання для кожної окремої поведінки, на основі якої здійснюється вибір та активізація дії в залежності від етапу маршруту. Кожен крок алгоритму можна умовно поділити на два етапи:

1. Аналіз ситуації у кожній точці, де знаходиться група БПЛА.
2. Переміщення групи БПЛА відповідно до вибраної поведінки.

Простір пошуку маршруту може містити зони, які поділяються на "Зону активної небезпеки", "Зону пасивної небезпеки" та "Цільову зону". Для формального опису простору пошуку маршруту пропонується застосувати елементи методу потенціальних полів. Загальна ідея методу полягає в русі об'єкта вздовж векторних ліній векторного поля, потенційна функція якого відображає конфігурацію перешкод та їх форму, а також ціль руху.

Простір пошуку маршруту охарактеризуємо масивом значень потенціальної функції $U(q)$. Розмір $U(q)$ дорівнює кількості елементів простору. Елементам масиву $U(q)$, які не входять у наведених вище зон, мають значення, що дорівнює 0.

Потенціальна функція може бути записана у вигляді

$$U(q) = U_{att}(q) + \sum_{i=1}^{n} U_{rep}^{i}(q), \qquad (1)$$

де $U_{att}(q)$ – потенціальна функція притягання,

$U_{rep}^{i}(q)$ – потенціальна функція відштовхування.

Для формального опису простору пропонується використовувати лише поняття потенціальної функції для подання простору у вигляді матриці значень.

Висновок. Таким чином, дискретна модель польоту підрозділу авіації, в якій політ розглядається як послідовне відвідування елементів простору, є багатовимірним масивом, кожному осередку якого приписується потенціальна функція цього елемента простору. Використовуючи різний крок дискретизації, можна розбити простір з необхідною точністю, що дозволить шляхом незначного збільшення вихідного масиву з більшою точністю описувати властивості областей простору і вибирати найбільш раціональні маршрути. Дана модель дозволяє обґрунтованості прийняття рішень та автоматизувати планування маршруту польоту групи БПЛА під час виконання цільового завдання.

Свердлюк Б.І. (ДУТ)
Каграманова Ю.К. (ДУТ)

NODE-RED – ІНСТРУМЕНТ АВТОМАТИЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Актуальність - інструменти no-code та low-code набирають більшу популярність. Вони мають різні цілі та допомагають з різними задачами. Проте якщо уявити універсальний інструмент для проектування та прототипування – першим на думку спадає Node-Red.

Постановка задачі – оцінка інструменту Node-Red для прототипування інформаційних систем та мереж.

Мета – Дослідити можливості Node-Red для автоматизації інформаційних систем та мереж

Node-Red — це потужний інструмент потокового програмування з відкритим кодом для автоматизації процесів в інформаційних системах. Він відноситься до Low code інструментів та дозволяє створювати взаємодії між пристроями, інформаційними системами, веб сервісами, API та програмами за допомогою графічного перетягування та об'єднання блоків (вузлів). Більшість коду створюється автоматично.

Node-Red можна встановити практично на будь чому локально у операційній системі Linux, або Windows, або на сервері. Також є можливість встановити його як Docker контейнер, npm пакет. Він складається з середовища виконання на основі Node.js,та запускається у веб-браузері.

Node-Red використовує технологію візуалізації на основі потоку (FBP) Це зручний для розуміння інструмент який розбиває проблему на дані, процеси, які працюють із цими даними, і мережу, яка з'єднує процеси разом.

Це чудовий інструмент для створення прототипів на початковій стадії проектування, або готових систем автоматизацій. За його допомогою можна створити: окрему функцію, набір нових функціональних можливостей або цілу програму від браузера до бази даних.

Node-Red активно використовується у створенні автоматизацій IoT пристроїв, створення чат ботів, створення логіки обробки звернень, листів, лідів CRM систем, для керування ПЛК, реле, системами освітлення, опалення та кондиціонування, обліку спожитої електроенергії.

Він набув неабиякої популярності у сфері IoT. За його допомогою можна моделювати фрагменти функціональності додатків між пристроями IoT, такими як датчики, камери та бездротові маршрутизатори. Проте він підходить для для виконання і багатьох інших задач.

Відкрита архітектура Node-Red дозволяє створювати вузли, написавши блок коду, або використовувати готові вузли.

Вузол — це блок коду, який може робити майже все, що завгодно. Наприклад парсити дані, читати веб форми, передавати API запити та багато іншого. Найкраща частина Node-Red полягає в тому, що він абстрагує базовий код, щоб дати розробнику високорівневе уявлення про те, що може робити Node. Але це не повний чорний ящик! Будь-хто може опублікувати власні вузли або працювати з авторами вузлів, щоб додати бажані функції до одного. На сьогодні в інвентарі Node-Red понад 4000 вузлів.

Палітра Node-Red включає стандартний набір вузлів, які є основною блоків для створення потоків:

Вузол «Введення» можна використовувати для запуску потоку вручну, натиснувши кнопку вузла в редакторі.

Вузол «Налагодження» можна використовувати для відображення повідомлень на бічній панелі налагодження у редакторі.

Вузол Функція дозволяє запускати код JavaScript для повідомлень, які пройшли через нього

Вузол «Змінити» можна використовувати для зміни властивостей повідомлення та встановлення властивостей контексту без необхідності звертатися до вузла Function

Вузол «Перемикач» дозволяє маршрутизувати повідомлення до різних гілок потоку оцінка набору правил щодо кожного повідомлення

Вузол «Шаблон» можна використовувати для створення тексту за допомогою властивостей повідомлення заповнити шаблон

Програмуючи за допомогою Node-Red, ви помітите його простоту. Як вказує назва no-code/low-code, кодування усувається, а програмування виконується інтуїтивно з мінімальною кількістю операцій, які потрібно використовувати.

FBP, типовий для Node-Red, може бути виконаний майже лише за допомогою операцій GUI. Редактор потоку Node-Red піклується про створення середовища виконання програми, синхронізацію бібліотеки, інтегроване середовище розробки (IDE) і підготовку редактора, щоб ви могли зосередитися на розробці.

Як представлено в об'єктно-орієнтованій розробці, зробити вихідний код загальним компонентом є однією з найважливіших ідей у розробці. У звичайній розробці на основі кодування кожен загальний компонент існує у функціях і класах, але в Node-Red вони існують як легкий для розуміння вузол (просто коробка). Якщо у вас немає вузла як загального компонента, який ви хочете використовувати, будь-хто може створити його негайно та опублікувати у всьому світі.

Висока якість — це справжня цінність потокового та візуального програмування. Кожен вузол, наданий як компонент, є повним модулем, який пройшов модульне тестування. У результаті автори програми можуть зосередитися на перевірці операції на рівні об'єднання, не турбуючись про вміст вузла. Це важливий фактор, який усуває людську помилку на єдиному рівні та забезпечує високу якість.

Node-Red — це програмне забезпечення з відкритим кодом. Тому його можна гнучко використовувати за ліцензією Apache2. Деякі розробляють власні сервіси на основі Node-Red, тоді як інші змінюють власний інтерфейс і розгортають його як вбудований. Як ми вже згадували раніше, ми також створили платформу, де ми можемо опублікувати наш власний розроблений вузол, щоб будь-хто міг ним користуватися.

Висновок: Node-Red — інструмент що може створювати автоматизації та проектувати взаємодію в мережах, IoT, пристроях, інформаційних системах. Його відкритий код та безкоштовність лише сприяють його популярності. Він по праву посідає одну з перших сходинок у ніші автоматизацій no-code та low-code інструментів.

Світайло К.В. (ВІТІ ім. Героїв Крут)
Березовський Д.В. (ВІТІ ім. Героїв Крут)

МЕТОД РОЗРАХУНКУ НИЗЬКОПРОФІЛЬНИХ АНТЕН З ПЛАНАРНИМ ТА СТРУМЕНЕВИМ ЗБУДЖЕННЯМ

У теперішній час велику роль в системі управління військами в Збройних Силах України, ведення військової розвідки, рішення народно-господарських задач набуває система, що базується на використанні безпілотних літальних апаратів. Такі системи організаційно складаються з двох основних частин: наземного комплексу управління і безпілотного літаючого апарату.

Одними з найважливіших елементів будь-якого радіоканалу являється антенні пристрої, котрі визначають працездатність системи управління в ланцюзі. Антенні пристрої безпілотних літальних апаратів у силу сфери їх використання, повинні відповідати наступним вимогам: по-перше, мати полусферну діаграму направленості (ДН) з круговою поляризацією випромінюючого поля, по-друге, мати високі масогабаритні показники, не порушуючи електродинамічні характеристики літаючого апарату. Ці вимоги в більшій мірі відповідають прості, надійні, малогабаритні низькопрофільні антени (НПА), як одне з нових направлень розвитку антенної техніки. Метою даної роботи є аналіз методів розрахунків низькопрофільних випромінювачів для наступної їх розробки і використання в системах радіозв'язку з БПЛА.

Теорія низькопрофільних випромінювачів (НПВ) може бути побудована на базі різних фізичних моделей, дві з яких знайшли найбільш ширше використання на практиці - це резонаторна модель і модель довгих ліній. Згідно резонаторної моделі НПА представляється у вигляді резонатора формою якого визначається конфігурацією верхньою пластиною. Периметр резонатору обмежуючого вертикальною поверхнею в вигляді магнітної стінки (поверхність, на якій $H_\tau^S = 0$ – дотична складова магнітного поля). Така модель достатньо просто дозволяє вирішувати внутрішню задачу електричними по визначенню структури поля в резонаторі. Однак через великі помилки в визначенні резонансних частот, вхідного опору за рахунок крайніх ефектів в антенах, на практиці не знайшла широкого використання. Фізична модель «довгої лінії» відноситься до НПА з простою конфігурацією верхньої пластини (прямокутною, квадратною, круглою). НПА з прямокутною (квадратною) верхньою пластиною показується у вигляді розімкнутого відрізка несиметричної смужкової лінії, збудженої планарним або струмовим (штирем через отвір в екрані) методами. Джерелами поля випромінювача виступають дві торцеві щілини, створені верхньою пластиною і екраном. НПА і її еквівалентна схема показана на рис.1.

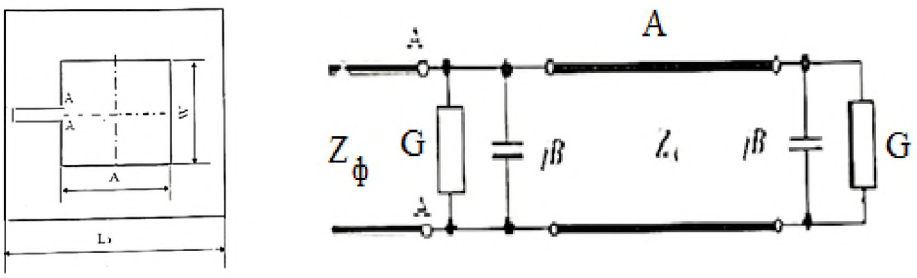


Рис.1 Низькопрофільна антена з прямокутньою верхньою пластиною

На Рис.1 введені наступні значення: А-А - точки підключення фідера у вигляді смужкової лінії; W - ширина верхньої площини; А - довжина верхньої площини; $L_в$ - розміри екрану.

Еквівалентна схема передбачає собою дві випромінюючі щілини з вхідною провідністю $Y = G + JB$ розділені відрізком лінії довжиною A з низьким хвильовим опором Z_A. Вхідна

провідність антени $Y_{вх}$ – результат складення провідності щілини на вході антени (точки А – А) і провідності перерахованої через відрізок смужкової лінії довжиною А.

$$Y_{вх} = G + jB + Y_A \frac{(G+jB)+jY_A tg\beta A}{Y_A + j(G+jB)tg\beta A}$$

де β- постійна поширення ЕМХ; $Y_A = 1/Z_A$ – провідність еквівалентної лінії; $G \approx W/120\lambda$ – активна частина провідності випромінювання щілини; $B \approx A/60\Lambda$, її реактивна частина; $\Lambda = \frac{\lambda}{\sqrt{\varepsilon_{еф}}}$ – довжина хвилі в смужковій лінії; $\varepsilon_{еф}$ – ефективна діелектрична активної провідності підложки.

Антена налаштована в резонанс, якщо її вхідна провідність являє речовою величиною, з формули перерахунку слідує умови резонансу:

$$tg\beta A = \frac{2Y_A B}{(G^2 + B^2 - Y_A^2)}$$

Отриманий вираз визначає резонансну довжину відрізка А лінії тобто верхньої пластини НПА з малим хвильовим опором Z_A, а також вхідний опір антени при її планарним збудженням.

$$Z_{вх} = \frac{1}{Y_{вх}} \approx \frac{1}{2G} \sin^2\left(\frac{\pi}{A}x\right) \approx 60\frac{\lambda}{W}$$

де: $G = \frac{1}{120} \cdot \frac{W}{\lambda}$

Довжина верхньої пластини А розраховується кілька менше пів довжини хвилі в смужкової лінії відповідно з виразом:

$$A = \frac{c}{2f} - 2\Delta$$

де: $\Delta = 0.412 \cdot h \cdot \frac{(\varepsilon_{еф}+0.3)\left(\frac{W}{h}+0.262\right)}{(\varepsilon_{еф}-0.258)\left(\frac{W}{h}+0.813\right)}$ – величина, враховуюча краєві ефекти на випромінюючих лініях.

При попередніх розрахунків чи при квадратній пластині НПА її ширина (W) обирається з вимог:

$$W = \frac{\lambda}{2\sqrt{\frac{1+\varepsilon}{2}}}$$

На рис. 2 показано результат теоретичного розв'язку вхідного опору НПА з квардратною верхньою пластиною при її живленні смужкової лінії.

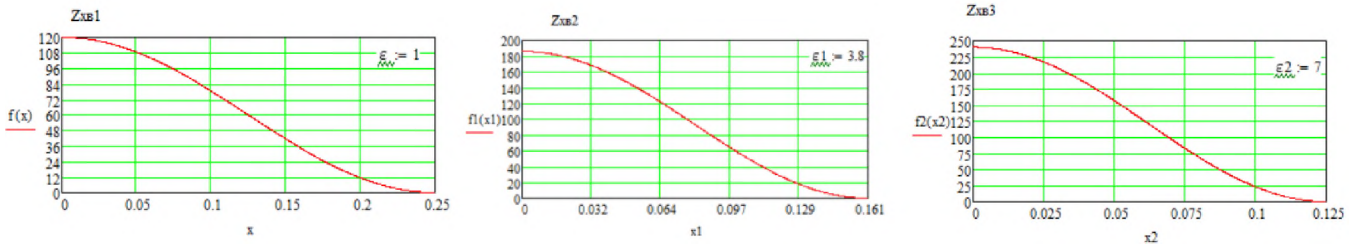


Рис.2 Вхідний опір низькопрофільної антени

Результат теоретичного досліджування НПА з квадратною верхньою пластиною показують, або при заповненню об'єму антен діелектриком суттєво змінюється її вхідний опір на вході антени, а також його розділенні по внутрішній області антени.

Отримані результати можуть бути використовують при розробці НПА з планарним або струменевим збудженням для використання в каналах радіозв'язку з БПЛА.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Банков С.Е. Антени супутникової навігації: аналіз характеристик низькопрофільних антен / Збірник наукових праць. Видавництво «Перо», 2014р.
2. Панченко Б.А. Мікрополоскові антени. Видавництво «Радіо і зв'язок», 1986р.
3. Захарьєв Н.Н., Леманський О.О., Турчин В.І. Методи виміру характеристик антен НВЧ. Радіозв'язок, 1985р. -368с

Сидоркін П.Г. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ ISO ТА NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) США, ЩОДО ОЦІНЮВАННЯ РИЗИКУ ВИТОКУ ІНФОРМАЦІЇ В КОМУНІКАЦІЙНИХ СИСТЕМАХ

Різноманітність методів оцінювання ризику витоку інформації в комунікаційних системах змушує нас ретельно дослідити переваги та недоліки деяких з них. На даний час більш застосованими в провідних державах світу є два стандарти, це - ISO та NIST (national institute of standards and technology) США. Обидва стандарти сприяють ефективній організації управління ризиками загроз для інформаційної системи і роблять роботу служб інформаційної безпеки більш чіткою. Тому метою даної статті є обгрунтоване орієнтування потенційних користувачів, щодо обрання найбільш корисного для них методу і забезпечити таким чином необхідний результат. Фахівці, які відповідають за організацію ІБ, керуються у своїй роботі стандартами, що розроблені авторитетними інституціями.

Формалізація даної роботи шляхом приведення її у відповідність одному чи декільком стандартам1 підсилює її ефективність, робить результати прогнозованими і є наслідком законодавчих вимог, що також впорядковують ці процеси.

Якщо чисельність ймовірних небезпек, або ризиків виникнення небезпек, величезна, тоді (як про це говорить практика) необхідна кількість стандартів і специфікацій3 повинна бути адекватною і пропонувати споживачеві різні методи та засоби дій4, спрямованих на досягнення максимального результату в короткій термін.

Одним з таких стандартів є ISO/IES 27005;2008, він входить у серію стандартів ISO/IEC 27000, присвячених менеджменту інформаційної безпеки5. Нові редакції даного документу видаються, як правило, щорічно, де враховуються нові виклики для ІС і нові засоби протистояння ним.

Як виявляється останнім часом дещо змінилися стосунки між споживачами Інтернет продукції. І на заміну атмосфері довіри в часи створення мережених протоколів, актуальних донині, у зв'язку, чи внаслідок інвестиційного розвитку, через появу більш «продвинутої» функціональності пріоритети змістилися в біг розробок нових можливостей та на шкоду рівню безпеки цих нововведень. Однак загрози для інформаційної безпеки постійно та швидко збільшуються. Їхніми носіями можуть бути: віруси, черві, різні «троянські коні», спроби сторонніх осіб імітувати з'єднання, порушивши таким чином цілісність захисної системи, можливі також крадіжки ідентичності. Звідси, побудова системи управління ризиками як найважливішої частини системи безпеки у кіберпросторі – це постійний процес прогнозування нових можливостей захисту ІС, мереж та додатків і ресурсів6. Сама мета і способи діяльності у світовій мережі, її взаємопов'язаність з усіма іншими операторами та необхідність використання тих плюсів, що вона їх додає користувачеві, водночас робить кожного з операторів вразливим для негативного впливу з боку інших операторів, конкурентів, суперників, супротивників. І складність у побудові системи безпеки полягає в її не перешкоджанні швидкому просуванню бізнесу, доступності послуг, що надаються. У світі бізнесу з його необхідністю постійного обміну інформацією внутрішній та зовнішній простори не мають чіткого розмежування, а периметр зони даної організації стає лише умовним. Тому використання в роботі різнорівневої організації діяльності з відповідними системами захисту на кожному з них значно ускладнить проникнення загроз та руйнацію ІС в цілому.

Висновки. Робота за стандартом NIST SP 800-30 дозволяє заглядати у подальшому майбутні ризики і готуватися до них заздалегідь. Тоді як робота за стандартом ISO/IES 27005;2008 дає можливість реагувати на нові виклики майже в on-line режимі, змінюючи процедури та методи управління ризиками в разі потреби.

к.ф.-м.н. Сімченко С.В. (ДУТ)

НАНОТЕКСТУРОВАНІ КВАНТОВІ ПРИЙМАЧІ ДЛЯ ОПТОВОЛОКОННИХ ЛІНІЙ ЗВ'ЯЗКУ

В зв'язку з бурхливим розвитком технологій та загальної інформатизації в усіх сферах діяльності суспільства надзвичайно актуальним є прикладне завдання по передачі значних обсягів інформації. Існуючі класичні технології передачі інформації такі як, використання коаксіального (мідного) кабелю або використання радіоканалу вже не здатні в повному обсязі забезпечити необхідної швидкості та якості сигналу. Також ці класичні способи мають ряд інших технічних недоліків. До яких можливо віднести вплив зовнішніх наводок, проблеми поширення та поглинання радіохвиль, спад сигналу пов'язаний з резистивним опором лінії.

В якості альтернативи якісної передачі інформації на значні відстаніостаннім часом все частіше використовують оптоволоконні лінії зв'язку. Такі лінії позбавлені основних недоліків, що мають класичні способи передачі інформації і мають істотні переваги при швидкісній передачі сигналу на значні відстані [1]. В останні роки оптичні лінії зв'язку по вартості конкурують з коаксіальними лініями та дозволяють обмінюватись інформаційними пакетами на швидкості ~ 1.5 Терабіт/с.

В якості передавача та приймача сигналу в оптоволоконних лініях використовують світло- та фотодіоди. Покращення електрофізичних параметрів та мініатюризація розмірів квантових приймачів для оптоволоконних ліній без сумніву є важливим та актуальним завданням.

В роботі показана можливість покращення чутливості фотоприймача сигналу завдяки створенню на його «активній» поверхні нанотекстурованого шару.

Для проведення досліджень нами використані кремнієві p-nпереходи площею 7х7мм^2(стандартні зразки сонячних елементів).

Порувату текстуру на поверхні яких отримували методом електрохімічного травлення.

Травлення відбувалось в розробленій нами фторопластовій комірці з платиновим кільцевим електродом (рис. 1). Джерелом живлення служив прецензійний блок на основі модуля KIS-3R33S. Струмова кінетика процесу травлення реєструвалась швидкодіючим АЦП та відображалась на екрані комп'ютера в режимі реального часу.

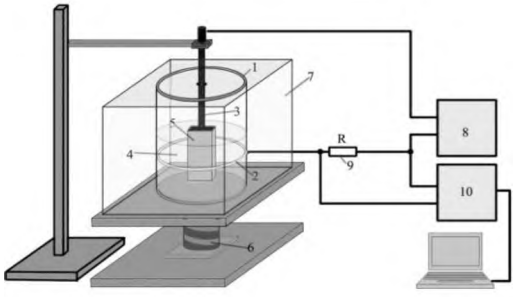


Рис. 1. Комірка для електрохімічного травлення
1-фторопластова ємність для електроліту; 2- кільцевий Pt електрод; 3- тримач зразка; 4- електроліт; 5- зразок; 6- підставка; 7- світлозахисний екран; 8- прецизійне джерело живлення; 9- опір; 10- блок АЦП.

В якості електроліту для травлення використовувалась 45% фтороводнева кислота, 40% соляна кислота, дистильована вода і 96% спирт в відношенні 1:1:1:1. Морфології отриманих поруватих структур досліджувались за допомогою растрового електронного мікроскопа REM-109. Товщина отриманих поруватих шарів для зразків становила від 40 до 80 нм, при розмірі пор 30-70нм.

Для отриманих зразків досліджувались спектральні характеристики. Результати вимірювання повного коефіцієнта відбиття (R), як функції довжини хвилі для сонячних елементів зображені на рис. 2.

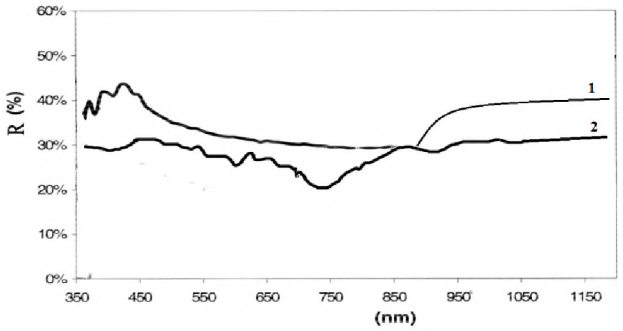


Рис. 2. Повний коефіцієнт відбиття як функція довжини хвилі для стандартного зразка (1); для зразка з поруватим покриттям (2)

Як видно з рисунка на зразках з текстурованою поверхнею спостерігається збільшення поглинаючої здатності, що свідчить про збільшення ККД перетворення таким фотоелементом. Збільшення поглинання падаючого на поверхню зразка випромінювання залежить від розмірів та геометрії створеної на поверхні текстури.

ВАХ створених нами фотодіодівпредставлені на рис 3. Крива 2 знята для квантових приймачів з поруватим шаром (пористість 55 %), крива 1 досліджена для фотоприймачів без поруватого шару. В обох випадках ВАХ досліджені для зразків площею поверхні 49 мм^2 при інтенсивності випромінювання 1000 Вт/м^2 і температурі 300К. Як видно з графіка значення струму короткого замикання в фотодіодах з поруватим шаром збільшується ~ 3 % порівняно з монокристалічним зразком таких же розмірів.

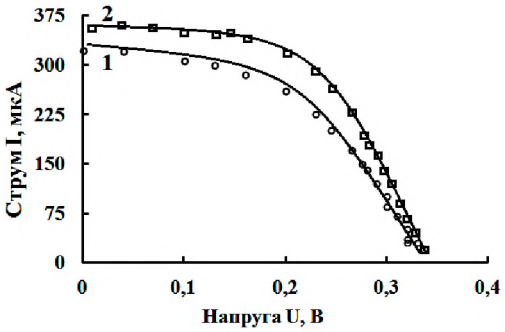


Рис. 3. Вольт-амперні характеристики сонячних елементів з поруватим шаром (2) та без поруватого шару (1) T=27^{0}C

Напруга холостого ходу для обох зразків практично не змінюється. Підвищення струму фотоприймача можна пояснити завдяки збільшенню активної площі поверхні поруватого шару. Збільшення площі поверхні дозволяє підвищити фото генерацію додаткових носіїв заряду у сформованому поруватому шарі.

Такий спосіб дає змогу без значних конструкційних змін фотоперетворювача покращити характеристики квантових приймачів для оптоволоконних ліній зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Волоконно-оптические системы передачи и кабели». Справочник. под ред. Гроднева И.И., Мурадяна А.Г., Шарафутдинова Р.М. и др.; М., Радио и связь, 1993.

2. Фотоэлектрические преобразователи на основе пористого арсенида галлия / А.И. Кирилаш, С.В. Симченко, В.В. Кидалов // Физическая инженерия поверхности. — 2012. — Т. 10, № 2. — С. 217–220.

Сінько В.В. (ВІТІ ім. Героїв Крут)
д.т.н. Могилевич Д.І. (ВІТІ ім. Героїв Крут)

МЕТОДИКА КОМПЛЕКСНОЇ ОЦІНКИ ПОКАЗНИКІВ НАДІЙНОСТІ ОБ'ЄКТІВ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ПРИ ВІДМОВАХ І ЗБОЯХ ПРОГРАМНИХ ЗАСОБІВ

Особливістю телекомунікаційного обладнання (ТКО) сучасних мереж зв'язку (МЗ) є те, що вони являються складними апаратно-програмними комплексами. Програмні засоби поряд з апаратною (технічною) частиною мають помітний вплив на надійність функціонування ТКО мереж зв'язку.

Метою дослідження є удосконалення науково-методичного апарату оцінки показників надійності ТКО мереж зв'язку при відмовах і збоях програмних засобів.

Методика призначена для розробки удосконаленого науково-методичного апарату – моделей оцінки надійності ТКО мереж зв'язку, що враховують обмежену надійність програмних засобів (ПЗ), різні способи часового резервування, характеристики контролю працездатності і відновлюваності програмних засобів, неповноту вихідної інформації. Моделі оцінки надійності ТКО дозволяють проводити кількісну оцінку впливу на надійність ТКО вказаних факторів з метою обґрунтування рекомендацій щодо зменшення впливу наслідків відмов і збоїв програмних засобів на процес функціонування мереж зв'язку.

Методика включає в себе сукупність взаємопов'язаних етапів, послідовне виконання яких призводить до досягнення поставленої мети.

На першому етапі методики визначаються основні фактори, які здійснюють найбільш суттєвий вплив на надійність функціонування ТКО МЗ у вказаних вище умовах. Вплив одних факторів (назвемо їх «агресивними») призводить до зниження рівня надійності об'єктів ТКО (недосконаліть ПЗ, збої та стійкі відмови програмних засобів, недостатня кваліфікація обслуговуючого персоналу, низька ефективність засобів контролю і діагностування ПЗ та ін.). При цьому відмови ПЗ можуть призводити до різних наслідків: одні викликають повне або часткове знецінення попереднього напрацювання (знецінені відмови), а інші викликають тільки затримку виконання завдання на час відновлення працездатності стану програмних засобів. Вплив інших факторів направлений на компенсацію (зменшення) впливу «агресивних» факторів з метою забезпечення нормального функціонування об'єктів (підвищення надійності ПЗ шляхом забезпечення його високої відмовостійкості і нечутливості до певних типів помилок та спотворень; використання різних видів резервування; зменшення вторинних втрат оперативного часу та ін.). В даному дослідженні основна увага приділена різним способам часового резервування для забезпечення нормального функціонування ТКО в умовах відмов і збоїв програмних засобів.

На наступних етапах методики здійснюється розробка науково-методичного апарату – побудова моделей оцінки надійності функціонування ТКО мереж зв'язку з урахуванням різних типів відмов програмних засобів та інших факторів, що найбільш суттєво впливають на досліджувані процеси. При цьому розглянуті два випадки: 1) при повній і 2) при обмеженій вихідній інформації.

На заключних етапах методики проводиться всебічний аналіз впливу різних факторів на показники надійності функціонування ТКО мереж зв'язку в умовах обмеженої надійності ПЗ (відмов і збоїв програмних засобів).

Висновки. Отже, запропонована методика враховує відмови і збої програмних засобів, різні способи часового резервування, характеристики контролю працездатності і відновлюваності ПЗ. Представлена методика дозволяє проводити кількісну оцінку показників надійності ТКО і ступінь їх відповідності заданим вимогам, виявляти «слабкі» місця та науково обґрунтовувати рекомендації щодо вибору шляхів і методів компенсації наслідків відмов і збоїв програмних засобів на функціонування ТКО мереж зв'язку.

к.т.н. Слонов М.Ю. (ВА ім. Є. Березняка)
к.т.н. Марилів О.О. (ВА ім. Є. Березняка)
к.п.н. Пісненко С.А. (ВА ім. Є. Березняка)

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА КІБЕРПРОСТОРУ НА ТЕРИТОРІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Умови функціонування телекомунікаційних мереж та кіберпростору на території російської федерації (рф) визначаються федеральним законодавством. Після анексії Автономної республіки Крим, початку війни на сході України та з поширенням антиросійських настроїв на Заході, агресор актуалізував проблему тотального контролю телекомунікаційних мереж та кіберпростору країни. Технічним рішенням даного питання стало впровадження удосконаленої системи технічних засобів для забезпечення функціонування оперативно-розшукових заходів, відомої як "СОРМ".

Характерною особливістю роботи з серверами розміщеними на території рф є фіксація всієї активності в кіберпросторі країни агресора місцевими правоохоронними органами. Нормативно-правовою базою для урядового контролю за телекомунікаційними мережами та кіберпростором на території рф став так званий "Пакеті законів Ярової", що був прийнятий в 2016 році та дозволив правоохоронним органам відслідковувати мережевий трафік. А постійне оновлення програмно-апаратних комплексів "СОРМ" потребує врахування даного фактору під час роботи з серверами розміщеними на території рф. Тому, опис функціонування можливостей "СОРМ" є актуальним завданням.

Аналізособливостей функціонування "СОРМ" в телекомунікаційних мережах та кіберпросторі рф передбачає опис питань про склад, структуру та функціональні можливості системи. Відповідно до зарубіжних відкритих наукових джерел інформації встановлено, що комплекси "СОРМ" дозволяють виконувати наступні дії: проводити збір інформації з доступом до неї правоохоронних органів рф у часі близькому до реального; зберігати інформацію про активність абонентів в телекомунікаційних мережах та кіберпросторі рф на термін близько трьох років; збирати інформацію з кіберпростору відповідно до завчасно визначених маркерів пошуку; аналізувати зібрану інформацію.

Обладнання комплексів "СОРМ" за функціональними можливостями умовно можна розділити на три основні частини: програмно-апаратні комплекси оброблення інформації; пристрої фіксації активності в телекомунікаційних мережах та кіберпросторі; канали обміну інформацією між програмно-апаратними комплексами та пристроями фіксації активності.

Аналогічні системи урядового контролю функціонують в інших країнах, а саме, в країнах ЄС (LawfulInterception), США (CommunicationsAssistanceforLawEnforcementAct), Білорусі та Казахстані. Відмінність російської "СОРМ" полягає в тому, що співробітники правоохоронних органів зобов'язані мати діюче судове рішення, але можуть використовувати функціонал системи без пред'явлення судового ордеру оператору зв'язку.

Комплекси "СОРМ" дозволяють акумулювати інформацію про мережеві ресурси до яких звертались абоненти, вести історію відвідування Інтернет сайтів та соціальних мереж. Фактично, "СОРМ" представляє собою державний аналог Інтернет-маркетингових аналітичних ресурсів.

Отже, система технічних засобів для забезпечення функціонування оперативно-розшукових заходів російської федерації має ряд характерних відмінностей від аналогічних систем інших країн. Комплекси "СОРМ" дозволяють здійснювати фіксацію та аналіз всього трафіку в телекомунікаційних мережах та кіберпросторі на території рф. В склад комплексів "СОРМ" входить апаратура оброблення, фіксації та передачі інформації, що циркулює в кіберпросторі на території рф. Врахування функціональних особливостей роботи комплексів "СОРМ" дозволить без обмежень використовувати сервери, що розміщенні на території рф. Невисвітленими залишаються питання врахування впливу сервісів VPN на функціонування "СОРМ" під час роботи в телекомунікаційних мережах та кіберпросторі рф.

Совік О.В. (ВІТІ ім. Героїв Крут)
Кокошинський В.В. (ВІТІ ім. Героїв Крут)
Прохорський С.І. (ВІТІ ім. Героїв Крут)
Гетьман А.В. (ВІТІ ім. Героїв Крут)

УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЮ ІНФРАСТРУКТУРОЮ ЗБРОЙНИХ СИЛ УКРАЇНИ: СТАН, ПІДХОДИ, ЗАДАЧИ І ПЕРСПЕКТИВИ

На підставі аналізу побудови системи управління електронними комунікаціями (СУЕК) ЗС України, а також оцінки практичної роботи органів управління і чергових змін ІТВ можливо зробити вирок про те, що завдання організаційного і технологічного управління електронними комунікаціями (ЕК) і їх елементами проводяться в неавтоматизованому або частково автоматизованому режимах.

Під управлінням ЕК розуміються цілеспрямовані дії, що пов'язані з плануванням, розгортанням (побудовою) та експлуатацією мереж, що роблять більш ефективним використання їх ресурсів.

Основними завданнями СУЕК протягом усього життєвого циклу є:

• розгортання і введення в експлуатацію мереж ЕК;

• здійснення процесу експлуатації мереж ЕК;

• розвиток мереж ЕК.

СУЕК повинна являти собою єдину систему обміну інформацією через керуючі додатки, автоматизацію завдань управління пристроями, огляд стану і продуктивності мережі, а також виявлення та визначення мережевих несправностей.

Одним з основних стандартів побудові СУЕК різнорідними територіально розподіленими мережами є концепція телекомунікаційної керуючої мережі Telecommunication Management Network (TMN), що запропонована Міжнародним союзом електрозв'язку (ITU). Концепція TMN викладена в рекомендаціях ITU серії M.3xxx і заснована на базових принципах управління відкритими системами, що визначені стандартом ISO 7498-4.

СУЕК, незалежно від характеристик об'єктів управління, повинна виконувати ряд функцій, які визначені міжнародними стандартами, узагальнюючими досвід застосування систем управління телекомунікаціями, а саме рекомендації ITU-T X.700 і близький до них стандарт ISO 7498-4, які ділять завдання системи управління на п'ять функціональних груп:

• управління конфігурацією мережі і ім'ям;

• обробка помилок;

• аналіз продуктивності та надійності;

• управління безпекою;

• облік роботи мережі.

Вибір СУЕК з урахуванням її адаптації під конкретну мережу ЕК – складна багатокритеріальна задача, тому вибір і побудова СУ повинні починатися з розробки технічного завдання на СУЕК.

Структура СУЕК повинна являти собою апаратно-програмні комплекси, що призначені для моніторингу стану, аналізу працездатності та управління апаратними та програмними засобами мереж ЕК.

СУЕК повинна здійснювати:

• моніторинг і аналіз функціонування програмно-технічних засобів функціональних та технологічних підсистем;

• організаційне та автоматизоване управління функціонуванням програмно-технічних засобів функціональних та технологічних підсистем.

СУЕК повинна забезпечувати:

• інтеграцію засобів адміністрування функціональних і технологічних підсистем;

• контроль параметрів функціонування апаратного та програмного забезпечення серверів і робочих станцій мереж ЕК;

• аналіз даних про функціонування підсистем і розподілених додатків;

• накопичення, аналіз і відображення результатів контролю стану і працездатності елементів мереж ЕК;

• своєчасне виявлення, локалізацію і управління усуненням несправностей;

• прогнозування критичних станів системи та запобігання виникненню відмов у роботі елементів мереж ЕК на ранній стадії;

• вироблення команд і сигналів управління технічними і програмними засобами підсистем в автоматичному і ручному режимах для прийняття рішення системним адміністратором;

• оптимізацію планування завдань обслуговування системи з урахуванням завантаженості ресурсів мереж ЕК;

• оптимальний розподіл загальних обчислювальних і комунікаційних ресурсів з урахуванням їх значущості в системі управління військами (силами) і зброєю;

• автоматизацію планування діяльності персоналу з управління функціонуванням при технічному обслуговуванні та регламентних роботах;

• реєстрацію та документування подій в мережах ЕК, дій адміністраторів з управління функціональними і технологічними підсистемами.

При реалізації зазначених та інших функцій в СУЕК доцільно використовувати:

способи моніторингу - активний, пасивний або їх комбінацію;

методи управління - централізований, децентралізований або їх комбінацію.

Найбільший інтерес представляє принцип побудови СУЕК, заснований на розгляді в тісному взаємозв'язку методів централізованого та децентралізованого управління, активного і пасивного моніторингу. У цьому випадку проводиться раціональний поділ завдань управління. Саме такий принцип пропонується для застосування в СУЕК ЗС України.

В основі СУЕК повинна лежати схема взаємодії "агента" з "менеджером". Спеціалізоване програмне забезпечення СУЕК повинне складатися з трьох окремих програмних компонентів - серверного, клієнтського і агентського програмних модулів, які забезпечують формування інформації для прийняття управлінських рішень.

На основі цієї схеми можуть бути побудовані системи практично будь-якої складності з великою кількістю агентів та менеджерів різного типу.

Підготовлена інформація в СУЕК формується за результатами моніторингу елементів мереж за напрямками: моніторинг послуг, системний моніторинг, ресурсний моніторинг, апаратний, моніторинг геопозиціонування інфраструктури, моніторинг витрат, моніторинг ефективності, пооперaційний моніторинг.

Завдання системи моніторингу СУЕК, критерії та показники її роботи повинні обиратися методом експертної оцінки, в залежності від місця і ролі мережі ЕК в системі управління військами (силами) та зброєю.

СУЕК ЗС України повинна розроблятися з метою досягнення кінцевої мети:

• підготовка інформації для прийняття управлінських рішень;

• доведення необхідної інформації до посадових осіб, які приймають рішення щодо управління системою;

• забезпечення необхідної готовності мереж ЕК до виконання задач за призначенням;

• забезпечення заданої якості послуг з інтегрованою оцінкою не нижче встановленої;

• оптимізації використання та збільшення реального завантаження ресурсів ЕК;

• перехід від ідеології контролю SLA до ідеології управління SLA;

• повний перехід на управління ризиками.

Ph.D Солодовник В.І. (ВІТІ імені Героїв Крут)
д.т.н. Науменко М.І. (ВІТІ імені Героїв Крут)
Пилипенко М.Г. (ВІТІ імені Героїв Крут)

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ПРОСТОРОВОЇ МОДУЛЯЦІЇ СИГНАЛІВ ІЗ РІЗНОЮ КІЛЬКІСТЮ АКТИВНИХ ПЕРЕДАВАЛЬНИХ АНТЕН

На теперішній час в умовах війни з російською федерацією (рф) якісне управління військами та зброєю набуло особливо важливого значення. Високий рівень інформаційного забезпечення управлінської діяльності стає визначальним чинником досягнення стратегічної та оперативно-тактичної переваги над противником. Якісна загальна ситуаційна інформованість дозволяє істотно підвищити ефективність бойового застосування сил та засобів, а також значною мірою вплинути на хід і результат операції (бою). Зазначене вимагає передачі великих об'ємів інформації – швидко, надійно та без спотворень.

Традиційні екстенсивні шляхи підвищення спектральної (СЕ) та енергетичної ефективності (ЕЕ) систем передачі вичерпали себе ще в минулому столітті. Внаслідок обстрілів з боку військ рф об'єктів критичної інфраструктури України словосполучення "дефіцит енергетичних ресурсів" вже не є загальним, теоретичним і не до кінця зрозумілим.

Для вирішення задач, пов'язаних зі створенням єдиного інформаційного простору з гарантованим наданням послуг зв'язку не тільки на пунктах управління, але і у відриві від них, використання безпроводових телекомунікаційних технологій є практично безальтернативним. Відомо, що застосування багатоантенних систем MIMO (Multiple Input – Multiple Output) сприяє істотному покращенню показників СЕ та ЕЕ, а також забезпеченню можливостей та умов обміну ЕЕ на СЕ.

Класичні методи просторової обробки сигналів мають ряд відомих недоліків. Забезпечуючи високі показники швидкості передачі інформації, методи просторового мультиплексування (Spatial Multiplexing, SMX) характеризуються низькою завадостійкістю та потребують високопродуктивних дороговартісних цифрових процесорів обробки сигналів у приймачі. Прості у декодуванні ортогональні просторово-часові блочні коди та їх частотні версії є енергетично ефективними, проте низькошвидкісними. Одночасно забезпечити високі показники рознесення та мультиплексування сигналів дозволяють Perfect-коди. На сучасному етапі розвитку схемотехніки практичне впровадження потужних "досконалих" кодів типу Perfect унеможливлюється через їх високу обчислювальну складність.

Підвищити СЕ та ЕЕ можливо завдяки введенню додаткових сигнальних вимірів, що забезпечують формування та передачу певної частини інформаційних біт, шляхом реалізації неявного інформаційно-керованого механізму перемикання стану активності (ON/OFF) допоміжних фізичних або віртуальних блоків трансляції. Прикладами таких сигнальних вимірів є просторовий (передавальні та приймальні антени, радіочастотні дзеркала, світловипромінюючі діоди), частотний (піднесучі), часовий (тактові інтервали), кодовий (коди розширення спектру, типи модуляції, матриці прекодування, дисперсійні матриці), кутовий (кути прибуття променів, види поляризації), енергетичний (потужність сигналів) тощо. Поєднання таких вимірів із використанням механізму ON/OFF дозволяє покращити ефективність і гнучкість реалізації систем без їх ускладнення з погляду практичної реалізації.

Зазначену концепцію впроваджено у широкий клас схем із індексною модуляцією (Index Modulation, IM) – методи передачі інформації, що полягають у поділі інформаційних біт на індексні та біти символів ансамблю сигналів із подальшою активацією складових блоків, що передають ці символи. Методи IM забезпечують альтернативні способи передачі інформації порівняно з традиційною передачею M-позиційних сигналів фазової (Phase Shift Keying, PSK) та квадратурно-амплітудної модуляції (Quadrature Amplitude Modulation, QAM), що дають можливість отримати енергетичний виграш (ЕВ) та/або виграш за СЕ з використанням меншої кількості ресурсів.

Світова телекомунікаційна спільнота виявила найбільшу зацікавленість методами

просторової модуляції сигналів (Spatial Modulation, SM), що дозволяють одночасно підвищити надійність та швидкість передачі інформації за рахунок введення додаткового просторового виміру сигналів.

Метод SM дозволяє передавати інформацію активуючи одну передавальну антену з N_T доступних із використанням тривимірного просторового-сигнального ансамблю. Таким чином, у кожному тактовому інтервалі передається $m = p_1 + p_2 = \log_2 N_T + \log_2 M$ біт, перша частина з яких ($p_1 = \log_2 N_T, N_T = 2^{p_1}$) називається індексною та визначає номер активної антени $\overline{N}_T$, а друга ($p_2 = \log_2 M$) – класичною та визначає модуляційний символ для передачі. Порівняно з класичним методом SMX типу V-BLAST, метод SM забезпечує компроміс за показниками CE/EE у залежності від розмірності MIMO, типів модуляції тощо; зниження обчислювальної складності приймача; високу EE; гнучкість налаштувань СРЗ та можливість роботи на одну приймальну антену (Multiple Input – Single Output, MISO); зниження рівня міжантенної інтерференції та спрощення вимог до синхронізації між передавальними антенами.

Метод SM сумісний із масивними MIMO, проте при $N_T > 8$ його ефективність є низькою, оскільки невелика кількість біт p_2 не може компенсувати втрати CE через деактивацію всіх доступних $\overline{N}_T$, крім однієї. Такий недолік усунено у методі розширеної SM (Generalized SM, GSM) із $\overline{N}_T > 1$, що є поєднанням методів SM та SMX.

Завадостійкий (Robust) варіант розширеної просторової модуляції RGSM також передбачає активацію $\overline{N}_T > 1$, проте для передачі одного і того ж символу *M*-PSK/QAM. Одночасна надлишкова передача одного модуляційного символу кількома передавальними антенами збільшує кількість його копій, що обробляються на приймальній стороні, забезпечуючи просторове рознесення. Метод RGSM не є конкурентним за показником CE, оскільки у кожному тактовому інтервалі передається $p = p_1 + p_2 = \lfloor \log_2 \left(C_{N_T}^{\overline{N}_T} \right) \rfloor + \log_2 M$ біт, де $\lfloor x \rfloor = \max \left\{ a \in \mathbf{Z} \middle| a \le x \right\}$, $\mathbf{Z}$ – множина цілих чисел; $C_{N_T}^{\overline{N}_T}$ – кількість комбінацій з N_T по $\overline{N}_T$, з очевидно невеликим внеском p_2. У завадостійкому методі просторової маніпуляції SSK (Space Shift Keying) та його аналогічних удосконаленнях здійснюється передача лише p_1 біт у просторовому вимірі, які є робастнішими, ніж p_2. Разом із тим, дослідження показали, що всі методи IM є найбільш ефективними при досягненні компромісу в кількості біт: $p_1 \approx p_2$.

Відомий метод GSM зі змінною кількістю $\overline{N}_T$ (Variable Active) – VA-GSM, в якому у таблиці асоціативності (формується у передавачі та відома приймачу) одночасно фігурують позиції із $\overline{N}_T = 1$ та $\overline{N}_T > 1$, проте в останньому випадку – для передачі одно і того ж символу *M*-PSK/QAM. Такий підхід дозволяє збільшити кількість біт $p_1 = \left\lfloor \log_2 \sum_{n=1}^{\overline{N}_T} \left(C_n^{N_T} \right) \right\rfloor$, та, відповідно, їх внесок у загальну CE.

Результати імітаційного моделювання у середовищі Matlab та експериментальні дослідження підтверджують високу завадостійкість методу VA-GSM порівняно із SM і GSM. Отриманий ЕВ (до 2 дБ при $P_{\text{п}} = 10^{-4}$) можливо використати для зменшення потужності передавача; збільшення дальності та/або швидкості передачі інформації; підвищення рівня достовірності прийому; зменшення вимог до чутливості приймача. Слід зауважити, що схеми передачі з IM (у тому числі, VA-GSM) не тільки визнано потенційними кандидатами для систем передачі інформації наступних поколінь на підставі теоретичного аналізу, а й підтверджено їх високу ефективність шляхом реалізації у конкретних технічних зразках.

Завдяки зазначеним перевагам методи на базі SM стали також компонентами багатьох сигнально-кодових конструкцій та можуть бути впроваджені у багатоантенні системи радіозв'язку Збройних Сил України й інших формувань цивільного та спеціального призначення.

д.т.н. Станкевич С.А. (НДІ ВР)
к.т.н. Кондратов О.М. (НДІ ВР)
к.т.н. Титаренко О.В. (НДІ ВР)
к.т.н. Стейскал А.Б. (НДІ ВР)
к.т.н. Масленко О.В. (НДІ ВР)
Щербань К.А. (НДІ ВР)

ОЦІНЮВАННЯ ВИДОВИХ МАТЕРІАЛІВ АЕРОКОСМІЧНОЇ РОЗВІДКИ ЗА ШКАЛОЮ NIIRS

Актуальність. Оцінювання якості видових матеріалів аерокосмічної розвідки є важливим та актуальним завданням для її планування та організації. Нині основними показниками оцінювання видової аерокосмічної розвідки вважаються повнота, достовірність та своєчасність, але на рівні окремих аерокосмічних знімків вони безпосередньо трансформуються на ймовірність виявлення та розпізнавання простих об'єктів. Саме цей показник і використовується для вирішення поточних завдань оцінювання видових матеріалів. Проте в арміях Північно-атлантичного альянсу якість видових матеріалів аерокосмічної розвідки оцінюється за допомогою системи експертних показників NIIRS (National Imagery Interpretability Rating Scale) [1]. Встановлення зв'язку цієї системи з прийнятими в Україні ймовірнісними показниками забезпечить сумісність одержуваних кількісних оцінок з прийнятими в НАТО і тим самим покращить планування аерокосмічної розвідки шляхом завчасного моделювання її результатів.

Отже, **метою** цього дослідження є забезпечення гармонізації прийнятих в Україні ймовірнісних показників оцінювання видових матеріалів аерокосмічної розвідки зі шкалою NIIRS, що полегшить планування розвідки та їх замовлення у країн-членівс НАТО.

Постановка завдання. Для досягнення мети потрібно провести науковий аналіз системи показників NIIRS, встановити статистичні закономірності їх взаємозв'язку з імовірністю виявлення простих об'єктів розвідки на аерокосмічних зображеннях та експериментально перевірити одержані результати для реальних аерокосмічних знімків з відомими значеннями NIIRS.

Основні положення. NIIRS є набором суб'єктивних критеріїв оцінювання якості зображення у вигляді бальної шкали від 0 до 9 [2]. Аналогічні шкали було розроблено для використання з багатоспектральними, інфрачервоними і радіолокаційними зображеннями. NIIRS широко використовується розвідувальним співтовариством США. Оцінки якості оптико-електронних і радіолокаційних зображень від розвідувальних супутників, літаків і БПЛА, включаючи Global Hawk, Dark Star, Predator та інші, анотуються у форматі NIIRS [3].

Показник NIIRS подає оцінку якості аерокосмічного зображення у звичній, зрозумілій та зручній формі і може бути оцінений візуально, без залучення вимірювань і розрахунків. Але класично NIIRS можна одержати лише постфактум за наявності зображення, тобто втрачається його прогнозна функція, дуже важлива при плануванні аерокосмічного знімання. Тому було запропоновано і впроваджено математичну модель GIQE (general image quality equation) для параметричного оцінювання NIIRS без залучення реального зображення [4].

Проте головним недоліком NIIRS як метрики якості аерокосмічних зображень є непристосовність до подальшого залучення в узагальнених моделях оцінювання ефективності та планування аерокосмічної розвідки, переважно імовірнісних [5]. Прийнята в Україні імовірнісна модель оцінювання видових матеріалів аерокосмічної розвідки базується на уточненій емпіричній формулі Живичина [6]. За нею ймовірності розпізнавання обчислюються для кожного рівня розпізнавання окремо. Всього застосовуються чотири рівні: виявлення об'єкта, розпізнавання до виду, до класу, до типу [7]. В цілому, ці рівні відповідають чотирьом прийнятим у НАТО – detection, distinguishing, recognition та identification, але всі вони є в єдиному показнику NIIRS залежно від його величини. Тому прямий перерахунок вектора ймовірностей в рівні NIIRS потрібно здійснювати за схемою "чотири до одного", а обернений буде неоднозначним. Взагалі, навіть у прямій моделі наявні

багато невизначеностей, пов'язаних із суб'єктивністю показника NIIRS, з розпливчатістю характеристик класів і типів об'єктів розвідки, з варіаціями геометричних і радіометричних властивостей аерокосмічних зображень та ін. В такій ситуації найбільш раціональним методом відновлення залежності між набором імовірностей та NIIRS багатовимірна регресія. Процедура визначення параметрів регресії описується схемою на рисунку.

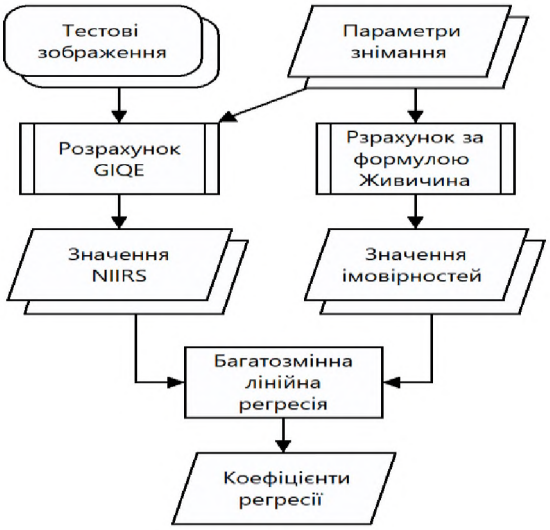


Схема визначення параметрів регресії

Моделювання здійснюється в два потоки – за розрахунком GIQE та за оцінюванням вектора ймовірностей розпізнавання. Далі будується багатозмінна лінійна регресія між ними. Всього було оброблено кілька сотень панхроматичних і багатоспектральних зображень від широко розповсюджених супутникових систем GeoEye-1, WorldView-2, WorldView-3, Pleiades-1, SuperView-1, Gaofen-2, RapidEye, Sich-2 та Sentinel-2 просторовою розрізненістю від 0,3 до 10 м з різноманітними об'єктами на них – спеціальною наземною технікою, літаками та вертольотами, кораблями. Після фільтрації викидів одержано багатозмінну лінійну регресію із середньоквадратичною похибкою 0,83, що є цілком прийнятним результатом.

Висновок. Встановлено статистичний взаємозв'язок рівня якості NIIRS аерокосмічного зображення з вектором імовірностей розпізнавання об'єкта, що можна використати для оцінювання очікуваного рівня якості NIIRS, навіть за відсутності реального зображення. Створений інструмент прогнозування рівня якості знімка за шкалою NIIRS розширює можливості планування видової аерокосмічної розвідки, забезпечуючи сумісність з чинним стандартом НАТО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. STANAG 7194 / AIntP-07 "NATO imagery interpretability rating scale (NIIRS)".
2. Irvine J.M. National imagery interpretability rating scales (NIIRS): overview and methodology. Proceedings of SPIE, 1997, vol. 3128, pp. 93-103. DOI: 10.1117/12.279081
3. Bai J., Sun Y., Chen L., Feng Y., Liu J. EO sensor planning for UAV engineering reconnaissance based on NIIRS and GIQE. Mathematical Problems in Engineering, 2018, vol. 2018, id. 6837014, 9 p. DOI: 10.1155/2018/6837014
4. Thurman S.T., Fienup J.R. Analysis of the general image quality equation. Proceedings of SPIE, 2008, vol. 6978, id. 69780F, 13 p. DOI: 10.1117/12.777718
5. Ребрин Ю.К., Станкевич С.А., Мосов С.П. Методы количественной оценки эффективности средств аэрокосмической разведки. К.: КИ ВВС, 1997, 262 с.
6. Станкевич С.А. Уточнення відомої емпіричної формули оцінки імовірності правильного дешифрування об'єктів на аерокосмічному зображенні. Збірник наукових праць Наукового центру ВПС України, 2004, вип. 7, с. 242-246.
7. Ребрин Ю.К. Оптико-электронное разведывательное оборудование летательных аппаратов. К.: КВВАИУ, 1988, 452 с.

Степанов В.О. (ВА м.Одеса)
Петренко Ю.А. (ВА м.Одеса)
д.т.н. Корчинський В.В. (ДУІТЗ)
к.ф.-м.н. Назаренко О.А. (ДУІТЗ)

ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ СИСТЕМ ЗВ'ЯЗКУ НА ОСНОВІ РОЗШИРЕННЯ СПЕКТРА ТАЙМЕРНИХ СИГНАЛІВ

Актуальність теми. В умовах радіоелектронного конфлікту доцільним є застосування таких систем радіозв'язку, що забезпечують високу завадостійкість і прихованість передавання інформації. Зазвичай, в таких системах застосовують широкосмугові шумоподібні сигнали, які можуть формуватися за допомогою різних методів розширення спектра бінарного сигналу [1]: псевдовипадковий перескок робочої частоти (ППРЧ); пряме розширення спектра за допомогою псевдовипадкових послідовностей (ПВП); лінійна частотна модуляція (ЛЧМ).

Такі методи розширення спектра сигналу розроблені лише для позиційних кодів і забезпечують енергетичну прихованість передавання сигнальних конструкцій в радіоканалі. Проте розвиток радіотехнічних засобів перехоплення широкосмугових сигналів потребують також ускладнення структури сигнальних конструкцій. Застосування більш складних шумоподібних сигнальних конструкцій дозволить підвищити їх структурну прихованість, що ускладнить розкриття структури сигналу у випадку перехоплення сеансу радіозв'язку засобами радіотехнічної розвідки.

Одним із способів підвищення структурної прихованості в порівнянні з розрядно-цифровим кодуванням є використання сигнальних таймерних конструкцій (ТСК) [2,3], інформаційна ємність яких більше ніж для розрядно-цифрового коду (РЦК). Таймерні сигнали є непозиційними, а їх структура залежить від параметрів пристрою кодування ТСК. Такі сигнали мають властивість завадостійкого коду, коригувальна здатність якого залежить від параметрів побудови ТСК. За рахунок зміни параметрів формування ТСК можна формувати різні ансамблі сигнальних конструкцій, що збільшує їх як структурну, так і інформаційну прихованість сигналів. Такі властивості ТСК обґрунтовують доцільність створення на їх основі шумоподібних сигналів. Зазвичай, методи розширення спектра сигналу розроблялися лише для позиційних кодів [1]. Існуюча невелика кількість наукових праць [2,3] по розширенню спектра непозиційних таймерних сигналів є ще недостатньою для їх практичного застосування, тому обґрунтованим є подальше дослідження в цьому напрямку. Тому метою даної роботи є аналіз методів синтезу шумоподібних таймерних сигнальних конструкцій на основі різних методів розширення спектра сигналу.

Основні положення. Відомі методи розширення спектра вузькосмугового сигналу засновані на перетворенні бінарної послідовності з тривалістю елементів Найквіста t_0. Відзначимо наступні переваги таймерних сигналів в порівнянні з РЦК: на заданому часовому інтервалі побудови $T_c = t_0 m$ можна сформувати більшу кількість реалізацій ТСК, тобто $N_{\text{рТСК}} > N_{\text{рРЦК}}$; завадостійке кодування на основі ТСК реалізується без додаткових перевірочних елементів; спільне використання завадостійких кодів на основи РЦК та ТСК зменшує ймовірність помилкового елемента на 3-4 порядки.

Розглянемо особливості побудови ТСК для того, щоб визначити відмінності розширення спектра непозиційних сигналів від РЦК. Принцип формування непозиційних ТСК [2,3] полягає у тому, що моменти модуляції імпульсів ТСК на відміну РЦК кратні не t_0, а деякому базовому часовому елементу Δ (де $\Delta = t_0/s$; $s = 1, 2, 3, ..., l$ – цілі числа). Тривалість імпульсів ТСК може бути менше інтервалу Найквіста, тобто $t_c = t_0 + k\Delta$ (де $k = 0, 1, 2, ..., s\cdot(n-2)$). Забезпечення більшої кількості реалізації N_p на інтервалі часу T_c порівняно з РЦК досягається за рахунок зменшення енергетичної відстані між ТСК, яка

залежить від значення $\Delta < t_0$. Елемент Δ впливає на завадостійкість і відносну швидкість передавання, що необхідно враховувати при виборі параметрів побудови ТСК. Загальна кількість реалізацій при ТСК [5]:

$$N_{\text{р}} = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}, \quad (1)$$

де i – кількість інформаційних моментів модуляції.

На рис. 1а надана реалізація ТСК на інтервалі $T_{\text{с}} = 4t_0$, $t_{\text{с}} = 4\Delta$. Бачимо, що реалізувати пряме розширення спектра сигналу на інтервалі t_0 за допомогою ПВП (рис. 1б) практично неможливо, тому що в межах комбінації ТСК тривалість імпульсу $t_{\text{с}} = t_0 + k\Delta$ може змінюватися. Це означає, що принцип прямого розширення спектра ТСК повинен враховувати часові інтервали побудови ТСК: Δ і $T_{\text{с}}$. Таким чином, ПВП повинна бути застосована до всього інтервалу $T_{\text{с}}$, що показано на часовій діаграмі (рис.1в). На рис. 1г надана часова діаграма розширення спектра ТСК за допомогою ППРЧ. При цьому методі розширення спектра сигналу частота носійного коливання f_1 може бути застосована до одного або кількох часових інтервалів Δ.

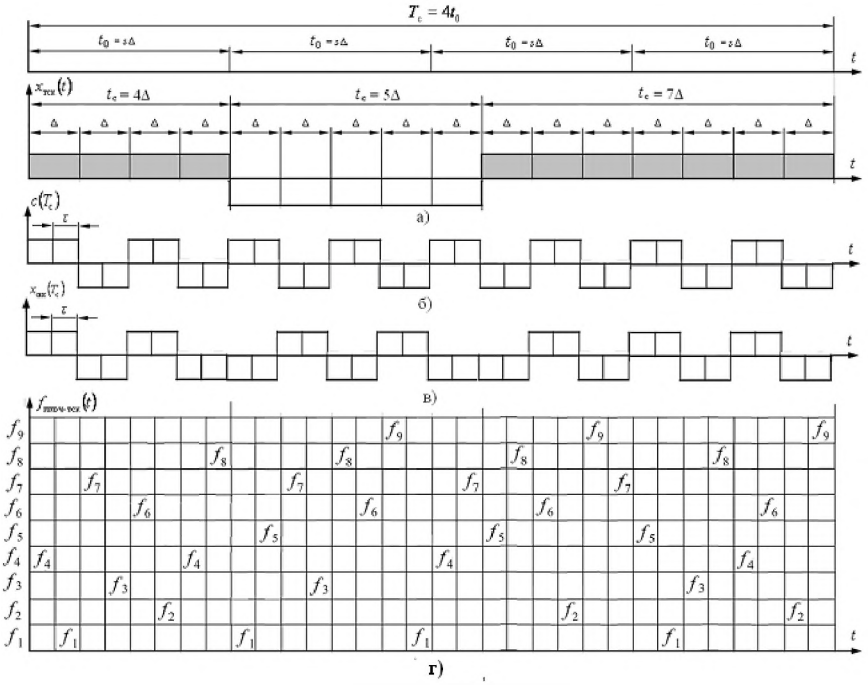


Рис. 1. Розширення спектра ТСК $x_{\text{ТСК}}(t_{\text{с}})$ за допомогою ПВП (в) та ППРЧ (г)

Висновки. Результати дослідження показують, що застосування шумоподібних таймерних сигналів дозволяє підвищити структурну прихованість та завадостійкість передавання інформації. При цьому ускладнюється алгоритм розширення спектра ТСК та потребує застосування нових методів прийому таких сигналів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев и др.; под ред. В.М. Борисова. – М.: Радио и связь, 2000. – 384 с.

2. Корчинський В.В. Конфиденциальная система связи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский// Вестник НТУ «ХПИ».– Харьков: ХПИ, 2013.–№ 16(989).–С.82-85.

3. Корчинський В.В. Повышение скрытности передачи на основе псевдослучайной перестройки рабочей частоты и таймерных сигналов / В.В. Корчинский // Вестник НТУ «ХПИ». Харьков: ХПИ, 2012.– № 66 (972).– С.63-67.

Табенський С.М. (НАДПСУ)

КІБЕРФІЗИЧНІ СИСТЕМИ, ЯК ІНСТРУМЕНТ В УМОВАХ СУЧАСНОЇ ВІЙНИ

Актуальність. Кіберфізичні (КФС) системи використовують вбудовані обчислювальні та цифрові мережі для моніторингу та контролю фізичних процесів, а також мають контури зворотного зв'язку, щоб фізичні процеси та обчислення могли впливати один на одного. Прикладами кіберфізичних систем є автоматична авіоніка, робототехніка, автономні автомобілі, розумні електромережі та системи керування процесами. На сьогоднішній день такі системи використовуються у найрізноманітніших галузях і сферах життя, серед яких важливим напрямком є впровадження таких систем у військову галузь, що дасть можливість зменшити час на прийняття рішень, цим самим підвищити ефективність виконання операцій та зберегти життя та здоров'я військовослужбовців.

Постановка задачі. Для забезпечення ефективного використання кіберфізичних систем під час сучасної війни важливим питанням є проаналізувати сучасний стан, переваги та перспективи їх впровадження.

Основні положення. Так на сьогоднішній день активно розвивається проект «Information Analysis for Multi-Domain Operations and Targeting Support», який на замовлення повітряних сил США досліджує можливість використання КФС в системах протиповітряної оборони, а також в безпілотних літальних апаратах в якості ефективної системи прийняття рішень. Справа в тому, що сучасне динамічне націлювання на ворожі об'єкти відбувається в дуже стиснуті показники часу, та дає мало часу для аналізу цілі, визначення найкращої зброї для ураження цілі та передбачає втручання людини для отримання команди на ураження. Таким чином не завжди вдається швидко здійснити ураження цілі навіть при її своєчасному виявленні. Тому повітряні сили реалізовують розробку технології для потреб центру повітряних операцій і бойового командування, які включають смертоносне, руйнівне та стійке націлювання за допомогою алгоритмічної війни, штучного інтелекту, машинної автоматизації та кіберфізичних систем.

Цей проект зосереджений на чотирьох технологічних областях: оптимізація; моделювання та імітація; аналіз робочого процесу; а також віртуальна та доповнена реальність. Крім того, він має три області застосування: багатогалузеві операції (або військові операції на суші, у повітрі, на морі, у космосі або в кіберпросторі); динамічне націлювання; і озброєння. Оптимізація спрямована на аналіз і покращення націлювання за допомогою визначення доступних ресурсів та вибору ідеальних доступних засобів зброї.. Мета полягає в тому, щоб скоротити час на планування місії, зменшити витрати на місію та підвищити рівень успішності місії.

Моделювання та імітація спрямовані на створення моделей, які імітують атаки на рухомі цілі, багатогалузеве командування та управління, а також використання сценаріїв динамічного націлювання, щоб визначити, як нові технології можуть формувати простір бою. Аналіз робочого процесу спрямований на використання методології робочого процесу для розуміння робочих процесів і результатів, заснованих на соціальній і технічній основі.

Віртуальна та доповнена реальність накладає інформацію з кількох різних джерел, щоб створити змодельовану багатовимірну картину поля бою, що дає змогу випробувати різні сценарії для підвищення ефективності місії та прийняття кращих рішень. Багатогалузеві операції спрямовані на інтеграцію операцій у кількох доменах і створення складних дилем для потенційних супротивників. Динамічне націлювання шукає способи атакувати цілі, які ідентифіковано надто пізно або не вибрано для дії вчасно, щоб включити їх до навмисного націлювання. Тим часом озброєння — це визначення кількості певного типу зброї, необхідної для завдання певного рівня ураження цілі.

Висновки. Таким чином використання кіберфізичних систем під час воєнних дій дає можливість набагато підвищити ефективність виконання бойових завдань та забезпечити збереження життя та здоров'я військовослужбовців.

Табенський С.М. (НАДПСУ)
Жук О.С. (НАДПСУ)
Ільницький М.М. (НАДПСУ)

ТЕХНОЛОГІЯ ДОВЕДЕННЯ РЕЗУЛЬТАТІВ КОНКУРСНОГО ВІДБОРУ ПІД ЧАС ВСТУПНОЇ КАМПАНІЇ ДО ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Актуальність. Відповідно до умов прийому для здобуття вищої освіти під час вступної кампанії заклади вищої освіти висвітлюють інформацію про етапи вступної кампанії (конкурсні пропозиції, результати вступних іспитів, рейтингові списки рекомендованих та зарахованих на навчання вступників) в Єдиній державній електронній базі з питань освіти (ЄДЕБО) та на офіційних веб-сайтах навчального закладу.

Проте вищі військові навчальні заклади (ВВНЗ) враховуючи безпекову складову та нерозголошенні персональних даних їх здобувачів освіти, не мають можливості висвітлювати інформацію у відкритих джерелах, що породжує в собі великі затрати часу та ресурсів при її персональному доведенні до кожного вступника.

Постановка задачі. Таким чином перед кожним ВВНЗ постає важливе питання, щодо реалізації оперативного, а головне персоналізованого та безпечного доведення інформації, щодо етапів вступної кампанії до кожного окремого вступника.

Основні положення. Серед головних вимог, при розробці даної технології є оперативність та зручність для вступника, а також можливість отримувати інформацію лише після проходження авторизації, для забезпечення надійності збереження інформації.

Зважаючи на сучасні тенденції використання месенджерів в якості джерела для отримання різноманітної інформації серед молоді, для забезпечення зручності користування, було прийнято рішення реалізувати технологію інформування на основі Telegram-бота.

Також такий підхід дозволяє забезпечити подвійну авторизацію на аналізі номера телефону з якого здійснюється запит, а також Telegram user id.

З метою безперебійної роботи сервіс рекомендується розміщувати на віддаленому віртуальному сервері з операційною системою - Linux. Також для забезпечення автоматизованого запуску роботи сервісу рекомендовано підключення системного менеджера Linux – systemd.

Дані з результатами надсилаються на сервер у вигляді Excel таблиці, слід звернути увагу, про відсутність у ній будь яких персональних даних, а ідентифікаторами є лише номер телефону та user id. Для забезпечення взаємодії між ботом та таблицею використовується Python-бібліотека Openpyxl.

Таким чином адміністратор після проходження окремого етапу вступної кампанії копіює дані в таблицю на сервері, а користувач в меню «Особистий кабінет» оперативно отримує інформування у вигляді push-повідомлення.

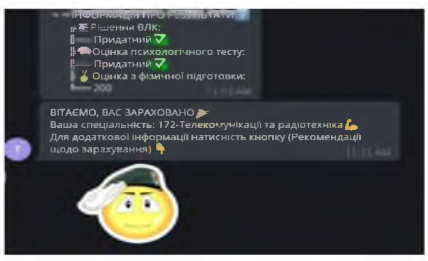


Рис. 1. Результат роботи Telegram-бота розробленого на основі технології.

Висновки. Представлена технологія дозволяє реалізувати засіб для оперативного, а головне надійного та безпечного доведення інформації, щодо проходження етапів вступної кампанії до кожного окремого вступника, що значно полегшує роботу приймальної комісії та забезпечує зручність проходження вступної кампанії.

Тихонов М.В. (КПІ ім. Ігоря Сікорського)
д.т.н. Могилевич Д.І. (ІСЗЗІ КПІ ім. Ігоря Сікорського)

АНАЛІЗ МЕТОДІВ ОЦІНКИ НАДІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ПРИ ОБМЕЖЕНІЙ ВИХІДНІЙ ІНФОРМАЦІЇ

Аналіз показав, що можливі два основні підходи, які дозволяють уникнути завищеної або заниженої оцінки показників надійності телекомунікаційного обладнання (ТКО) при обмеженій (неповній) вихідній інформації.

В основі першого підходу лежать методи, що використовують сімейство параметричних розподілів і базуються на тій чи іншій інформації щодо закону розподілу $F(x)$. Всі відомі в теорії надійності параметричні розподіли визначаються завданням скінченного числа параметрів. Ці сімейства використовуються, як правило, для апроксимації невідомої функції розподілу $F(x)$.

При відсутності необхідної інформації для вибору й обґрунтування виду закону розподілу $F(x)$ використовується другий підхід, заснований на непараметричних методах оцінки надійності. Цей підхід займає усе більш помітне місце в задачах випробувань на надійність систем та їхніх елементів, що пояснюється вихідними умовами, які лежать в їх основі. Вони дозволяють відмовитися від допущень щодо конкретного виду закону розподілу випадкових величин, значення яких підлягають обробці для наступного прийняття рішення.

При реалізації другого підходу є дві можливості:

а) припустити фізично виправданий напрямок динаміки розвитку системи («старіння», «омолодження») і віднести функцію розподілу $F(x)$ до деякого класу непараметричних розподілів, наприклад, до класу «старіючих» або до класу «молодіючих» розподілів;

б) не приймати взагалі будь-яких припущень щодо функції розподілу $F(x)$.

Прикладом реалізації першої можливості є введення й дослідження класу непараметричних розподілів $H(r,s)$, де r і s – будь-які числа, такі що $0 \le r < s \le +\infty$. Клас розподілів $H(r,s)$ визначається таким чином: у нього включаються ті й тільки ті розподіли $\overline{F}(t) = \exp(-\Lambda(t))$, для яких функція $\Lambda(t)/t^r$ є зростаючою, а функція $\Lambda(t)/t^s$ – спадаючою, де $\Lambda(t)$ – функція витраченого ресурсу на інтервалі часу $[0,t]$: $\Lambda(t) = \int_0^t \lambda(x)dx$. Таким чином, клас непараметричних розподілів $H(r,s)$ складається з тих розподілів, для яких функція ресурсу $\Lambda(t)$ має степеневий порядок росту з граничними значеннями параметрів r і s. Друга з можливостей реалізації непараметричних методів для оцінки надійності в умовах апріорної невизначеності заснована на тому, що відносно функції розподілу $F(x)$ не приймається взагалі будь-яких припущень. Цей підхід може бути використаний в тих випадках, коли в силу багатьох причин не має достатніх підстав навіть для того, щоб віднести досліджуваний об'єкт до класу «старіючих» або «молодіючих». Можливо лише припустити, що відоме тільки значення функції розподілу $F(x)$ і будь-яка інша корисна інформація про неї відсутня.

Висновки. На етапах проектування, розробки та експлуатації технічних систем, як правило, недостатньо вихідної інформації для достовірної оцінки показників надійності ТКО. Наявність невизначеності (неповноти) вихідної інформації обумовлено тим, що в багатьох випадках неможливо отримати достатньо великий об'єм вибірки випадкових величин, що характеризують безвідмовність, ремонтопридатність та процес функціонування ТКО, необхідний для оцінки узгодженості теоретичного та статистичного розподілів. Ця важлива особливість визначає ті труднощі, які доводиться долати при оцінці надійності для отримання результатів розрахунку, прийнятних для використання в інженерній практиці. Проведений аналіз методів показав, що для оцінки надійності ТКО з комбінованим резервом часу доцільно застосувати непараметричний метод, при якому відоме тільки значення функції розподілу $F(x)$, але будь-яка інша корисна інформація про неї відсутня.

к.т.н Ткаченко А.Л. (ВІТІ ім. Героїв Крут)
Сергієнко А.В. (ВІТІ ім. Героїв Крут)
Драглюк О.В. (ВІТІ ім. Героїв Крут)
Краснобокій А.В. (ВІТІ ім. Героїв Крут)

ШЛЯХИ УДОСКОНАЛЕННЯ КОМПЛЕКСНИХ АПАРАТНИХ ЗВ'ЯЗКУ ЗА РЕЗУЛЬТАТАМИ ЇХ ЗАСТОСУВАННЯ ПРИ ВІДСІЧІ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Актуальність. З початком повномасштабного вторгнення російської федерації в нашу країну почали різко змінюватись форми та способи ведення операцій (бойових дій). Застосування новітніх видів озброєнь та техніки, нових видів військових з'єднань та формувань вимагає й перегляду способів організації зв'язку для забезпечення відповідних процесів управління. Одним з варіантів вирішення поставлених питань з організації зв'язку стало швидке переобладнання та передача у загальновійськові з'єднання комплексних апаратних зв'язку (далі – КАЗ), що дозволило оперативно забезпечити пункти управління новостворених з'єднань та об'єднань такими сервісами зв'язку, як передача даних, відкрита та захищена телефонія, сервісами доступу до інформаційних систем відповідно до їх призначення, тощо. Разом з цим виявився й ряд недоліків, які потребують врахування та виправлення при подальшому застосуванні КАЗ.

Мета дослідження. На основі досвіду застосування комплексних апаратних зв'язку в організації зв'язку в операціях (бойових діях) дослідити можливі шляхи їх удосконалення.

Виклад основного матеріалу. Розвиток інформаційних та телекомунікаційних технологій на сучасному рівні характеризується мініатюризацією елементної бази, а отже зменшенням розмірів кінцевих пристроїв, що здійснюють обробку та передачу інформації. Застосування їх у військовій сфері дозволяє суттєво зменшити кількість сил та засобів, що забезпечують розгортання та експлуатацію комунікаційних вузлів різного рівня та призначення. Як результат цьому стала поява комплексних апаратних зв'язку, які призначені для забезпечення сервісами зв'язку, доступу до інформаційних (автоматизованих) систем службових осіб органів управління різних ланок шляхом об'єднання та використання різних родів та видів зв'язку та їх застосування в інформаційно-комунікаційних мережах ЗС України.

Недоліком КАЗ стало їх застосування на старих зразках автомобільного шасі – типу ЗІЛ-131 та контейнерів універсальних не герметичних (КУНГ) ще радянського зразка. Масивність конструкції, наявність антено-щоглових пристроїв в складі КАЗ несуть досить великі демаскуючі ознаки при її розміщенні на пунктах управління з'єднань та при використанні противником сучасних засобів розвідки, таких як БПЛА, дій ворожої агентури, а отже досить легко виявляються та піддаються вогневому впливу. В результаті таких дій противника, необхідне обладнання КАЗ почали виносити в захищені споруди, а самі апаратні після демонтажу обладнання відправляти за межі дії відповідних вогневих засобів противника.

Як вихід з ситуації, що склалася є необхідність дослідження питання заміни автомобільного базового шасі КАЗ з ЗІЛ-131, КАМАЗ на більш сучасні на базі мікроавтобусів, фургонів, пікапів тощо, а засоби зв'язку, що входять до складу КАЗ, робити модульного виконання контейнерного типу, з можливістю їх легкого демонтажу, переміщення силами екіпажу та розміщення у захищених спорудах, в яких знаходяться відповідні пункти управління. Окремо має розглядатись питання складу засобів зв'язку.

На даний час застосування цивільних транспортних засобів в інтересах організації зв'язку в підрозділах, які виконують бойові завдання, має широке використання.

Кожен підрозділ формує апаратну зв'язку в залежності від наявного того чи іншого транспортного засобу, виконуємих задач, а також наявності у підрозділі засобів зв'язку.

Реальними варіантами є наступні: мікроавтобус фольксваген Т4, Крафтер або мерседес Віто, Спринтер із засобами зв'язку: ТК-2, телекомунікаційна стійка, а також

електрогенератор, автомобіль має можливість вміщувати даний комплект обладнання плюс обслуговуючий персонал.

Даний варіант найчастіше використовується на пунктах управління різних ланок управління для організацій телефонного зв'язку та передачі даних. В той же час, за результатами досвіду, в підрозділах інших видів (родів військ) зустрічаються варіанти використання як інших транспортних засобів так і іншого комплекту обладнання:

пікап – ретранслятор, комплект супутникового зв'язку, УКХ радіостанція;

мікроавтобус – телекомунікаційний комплект, комплект супутникового зв'язку, станції широкосмугового доступу, УКХ, КХ радіостанції; інше.

Отже, важко визначити типовий комплект комплексної апаратної зв'язку в сучасних умовах ведення бойових дій – все залежить від сукупності факторів виконання завдань та наявності обладнання.

За досвідом виконання завдань з організації зв'язку у підрозділах є декілька варіантів вирішення питання, щодо створення апаратних зв'язку на цивільному (або замаскованого під цивільний) автомобільному шасі підвищеної прохідності.

Один із варіантів є визначення базової комплектації апаратної зв'язку, що повинна задовольняти основні (базові) потреби в сервісах зв'язку, такі як: відкриту/закриту телефонію та передачу даних. Апаратна повинна мати можливість, за рахунок встановлення додаткового обладнання, нарощувати свої можливості щодо надання сервісів зв'язку.

Іншим варіантом є конструкторське (збірне) рішення, яке має на меті можливість встановлення засобів зв'язку за вибором, які є в наявності та/або відповідають виконанню певних задач в підрозділі, враховуючи особливості умов бойового застосування.

Даний варіант передбачає, що в апаратній зв'язку будуть проведенні роботи по забезпеченню електроживленням установленої апаратури, будуть передбачені місця для встановлення та кріплення контейнерів з телекомунікаційним обладнанням, будуть встановлені інші необхідні засоби зв'язку, такі як УКХ радіостанція (за необхідністю), у якої антена буде замаскована під цивільну автомобільну антену. Кріплення повинно дозволяти швидке встановлення та швидкий демонтаж телекомунікаційного контейнера.

Альтернативним може вважатися варіант, який буде сформований за результатами надання відповідних вимог споживачами апаратної у видах (родах) військ (сил), з урахуванням їх потреб, а також умов, в яких КАЗ буде використовуватись, що, в подальшому, надасть можливість виявити типовий склад комплекту засобів зв'язку для підрозділів видів, окремих родів військ ЗС України. Варіант вибору складу комплексу засобів зв'язку споживачами представлений в таблиці нижче.

тип КАЗ МТ / склад комплексу	тип-1	тип-2	тип-3	тип-4	тип-5	тип-6	тип-7
автомобільна радіостанція транкінгового зв'язку	+	+	+	+	+	+	+
УКХ радіостанція, яка працює в діапазоні 30 – 512 МГц	+	+	+	+	+	+	-
ССЗ	+	+	+	-	-	-	+
стільниковий модем	+	+	+	-	-	-	-
телекомунікаційний комплект у контейнерному виконанні	+	+	-	-	-	-	-
…	…	…	…	…	…	…	…
апаратура спеціального зв'язку	+	+	+	-	-	-	-
телефонний апарат	+	+	-	-	-	-	-
Notebook	+	-	-	-	-	-	+

Особливу уваги слід приділити системі електроживлення, яка має задовольняти всі варіанти, які пропонуються та повинна забезпечувати функціонування апаратної автономно,

як на стоянці, так і під час руху, а також мати можливість здійснювати живлення засобів зв'язку та обладнання апаратної від зовнішньої однофазної мережі напругою 230 В та частотою 50 Гц (основне мережа електроживлення).

Пропонуються наступні автономні джерела електроживлення:

окремий електрогенератор потужністю, що забезпечує роботу засобів зв'язку апаратної та додаткового обладнання з можливістю його роботи на борту та/або винесеного не менше чим на 20 метрів;

джерело безперебійного електроживлення (з можливістю підзарядки від електрогенератора та зовнішньої електромережі) для живлення обладнання апаратної;

інвертор для живлення автомобільної транкінгової станції під час руху бази;

джерело безперебійного живлення в контейнерному виконанні (з можливістю підзарядки від електрогенератора та зовнішньої електромережі).

Вимоги, які повинні бути враховані до системи електроживлення.

Паливна система електрогенератора розраховується на використання того ж типу пального, що й паливна система транспортної бази.

Акумуляторні батареї резервного електроживлення забезпечують безперебійну роботу засобів зв'язку та обладнання апаратної під час переходу з одного виду електроживлення на інший. Час роботи обладнання апаратної від акумуляторних батарей резервного електроживлення повинно бути не менше 4 (чотирьох) годин.

Джерело безперебійного живлення в контейнері повинно забезпечувати живлення телекомунікаційного комплекту та інших телекомунікаційних складових за межами апаратної не менше 6 (шести) годин.

У нормальному режимі повинна виконуватися подача електроживлення із основної мережі електроживлення. У разі переривання електроживлення на основному вводі повинно відбуватися автоматичне перемикання на акумуляторні батареї резервного електроживлення. Після відновлення параметрів мережі повинен відбуватися зворотний перехід на основну мережу.

Конструкцією засобів автоматичного включення резервного живлення повинна бути передбачена можливість ручного перемикання між джерелами живлення.

В складі апаратної повинна бути передбачена звукова та світлова сигналізація, яка сповіщає про перемикання електроживлення апаратури на акумуляторні батареї резервного електроживлення.

Всі розетки у апаратній, від яких буде здійснюватися живлення засобів зв'язку та обладнання, повинні бути з заземленням.

Шафа розподільна повинна забезпечувати розподіл електроживлення для окремих елементів комплексу засобів зв'язку та системи життєзабезпечення, а також захист ліній при коротких замиканнях та перевантаженнях, для нечастих оперативних включень та відключень електроживлення навантажень.

Комплект заземлення повинен забезпечувати зручне та швидке розгортання заземлюючого контуру апаратної та захист особового складу, засобів зв'язку та обладнання апаратної від ураження електричним струмом.

Висновки. Застосування сучасних автомобільних базових шасі в КАЗ дозволить покращити показники: мобільності системи зв'язку та інформаційних систем, оскільки сучасні базові шасі є більш швидкісними та ефективнішими за витратами ресурсів; розвідзахищеності, шляхом зменшення кількості демаскуючих факторів, а, отже і зменшення можливих людських втрат. Використання в складі КАЗ засобів зв'язку контейнерного типу дозволить оперативно розгортати відповідні пункти управління у визначених місцях, нарощувати їх відповідно до завдань, ланки управління, тощо. При прийнятті рішень на підготовку пропозицій щодо заміни транспортної бази слід дослідити питання оптимального складу екіпажу КАЗ, а також місця їх роботи та відпочинку.

Фесенко О.Д. (ВІТІ ім. Героїв Крут)
Гриценок К.М. (ВІТІ ім. Героїв Крут)

АВТОМАТИЗАЦІЯ ПОШУКУ АРХІТЕКТУРИ НЕЙРОНИХ МЕРЕЖ НА ЕТАПІ ПРОЕКТУВАННЯ НА ОСНОВІ АЛГОРИТМУ WANN.

Актуальність. На сьогодні існує потреба у розробці та інтегрування систем моніторингу обстановки в реальному часі для таких задач як комп'ютерний зір, розробка та проектування інтелектуальних автономних систем навігації наземних роботів чи безпілотних літальних апаратів (БПЛА). Відповідно з'являється необхідність в оптимізації процесу пошуку необхідної архітектури нейронної мережі для вирішення цільової задачі. Оскільки як правило для навчання розробленої моделі витрачається досить значний проміжок часу та ресурси, що ускладнює процес інтеграції.

Тому пропонується розглянути принципово новий алгоритм автоматизації пошуку архітектури нейронних мереж Weight Agnostic Neural Networks (WANN) [1,2].

Алгоритм агностичних нейронних мереж WANN це нова адаптивна нейромережа, робота якої полягає в процесі пошуку архітектури та навчання методом підбору структури нейромережі (кількість і розташування нейронів), оптимізація гіпер параметрів.

На рис. 1 показано порівняння складності класичної повно зв'язної нейромережі (зліва) і нової структури нейромережі в результаті методу підбору (праворуч).

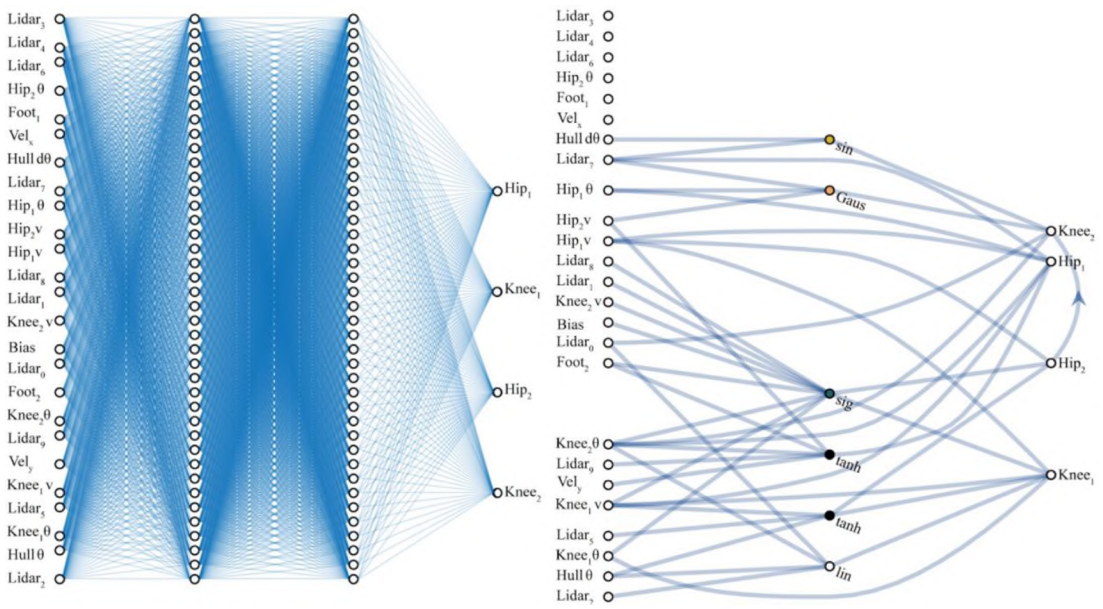


Рис. 1. Кінцевий результат оптимізації структури нейромережі за алгоритмом WANN.

На відміну від класичних рішень, при застосуванні WANN здійснюється оптимізація структури мережі, тому в якості додаткової цілі відбувається процес мінімізації числа нейронів.

Реалізація алгоритму WANN поділяється на наступні етапи:

1. Пошук топології.
2. Пошук оптимального правила навчання.

Перший етап алгоритму WANN полягає в процесі пошуку початкової архітектури нейромережі WANN, тобто застосовується алгоритм Topology search algorithm (TSA). Суть якого полягає в створені вхідної вибірки тривіальних нейромережевих структур (блок 1 на рис. 2). Наступним кроком додається новий нейрон в існуючу структуру створеної нейромережі, (блок 2 рис. 2), далі відбувається процес з'єднання нейрона з випадковим іншим нейроном (блок 3 рис. 2), а також змінюється функція активації в нейроні – блок 4, що описується нижче в рівнянні (1).

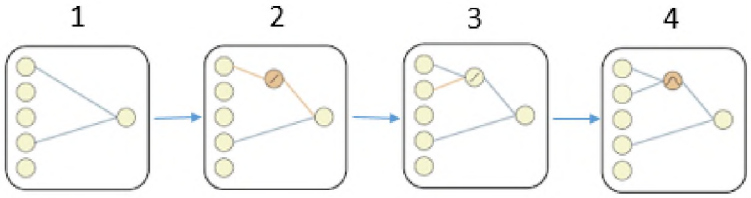


Рис. 2. Етапи вибору структури нейромережі на основі алгоритму WANN

$$A(S_i) = (S_1(T_{Ri:i}), S_2(N_i + N_{Ri:i}), S_3(f_{Ri:i})), \quad (1)$$

де $A(S_i)$ - функція створення первинної вхідної вибірки структури нейромережі, T_{Ri}- вузол формування структури нейромережі як процес випадкового розподілу, $(N_i + N_{Ri:i})$ −процес зєднання вибраного нейрона з нейроном вибраним як процес випадкового розподілу, f_{Ri} – вибір функції активації нейрона.

На рис. 3, показано повний процес вибору структури та навчання нейромережі WANN, який заснований на правилах генетичного алгоритму.

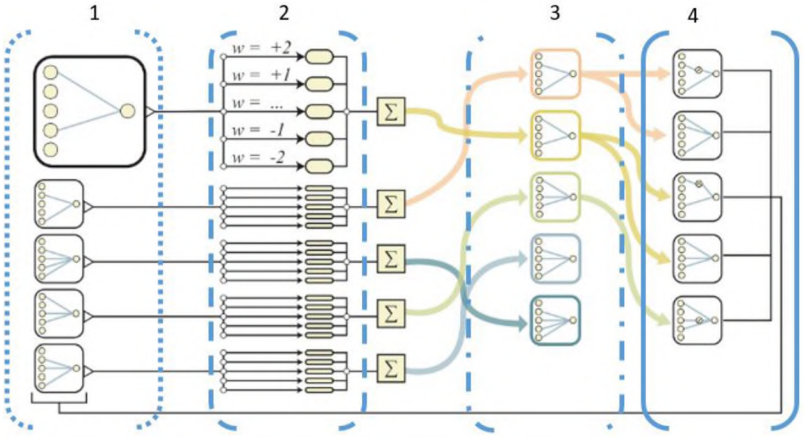


Рис. 3. Алгоритм WANN на правилах генетичного алгоритму.

У першому блоці рис. 3 відбувається процес визначення початкової популяції мінімальних топологій нейронної мережі, у блоці – 2 кожна створена мережа оцінюється за кількома тестовими випробуваннями, призначається різне значення вагових коефіцієнтів *W*. В блоці – 3 відібрані нейромережі структуруються в залежності від їх продуктивності і складності. Далі в наступному блоці створюється нова популяція шляхом варіювання топології мереж з найвищим рейтингом які вибираються ймовірнісним шляхом відбору на основі генетичних алгоритмів.

Таким чином перевага застосування такого алгоритму є значне зменшення кількості нейронів в мережі (так як залишаються лише найбільш важливі з'єднання), що збільшує швидкодію нейромережі та часові затрати щодо вибору оптимальних гіпер параметрів нейронної мережі .

Напрямком подальших досліджень є розробка методики управління міні – БПЛА в мережах FANETs (Flying Ad-hoc Networks) з урахуванням особливостей організації каналів управління і зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фесенко О. Д. Експериментальний аналіз застосування нейронних мереж для керування траєкторією польоту БПЛА / О. Д. Фесенко, Р. О. Бєляков, Г.Д. Радзівілов, В.С. Гулій // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2020. - Вип. 1. - С. 97-112.

2. Adam Gaier, David Ha, «Weight Agnostic Neural Networks» *[Submitted on 11 Jun 2019 (v1), last revised 5 Sep 2019 (this version, v2)].*

Фесенко О.Д. (ВІТІ імені Героїв Крут)
Ковальчук О.О. (ВІТІ імені Героїв Крут)
Терещенко О.М. (ВІТІ імені Героїв Крут)

МЕТОД МІНІМІЗАЦІЇ ВІДХИЛЕННЯ ТРАЄКТРОРІЇ БПЛА ПІД ЧАС ЗНИКНЕННЯ СИГНАЛУ ГЛОБАЛЬНОЇ СИСТЕМИ НАВІГАЦІЇ НА ОСНОВІ ФІЛЬТРАЦІЇ МАДЖВІКА.

Постановка завдання. У зв'язку із тим, що потреба у застосуванні безпілотних літальних апаратів (БПЛА) під час війни значно зростає, разом з тим відомо, що противник як правило застосовує технологію радіоелектронної боротьби (спуфінг атаки) проти БПЛА, що може стати критично для виконання місії польоту та втрати БПЛА. Тому відповідно підвищується необхідність розробок алгоритмів систем управління БПЛА в автономному режимі польоту незалежно від наявності сигналів глобальних систем позиціювання.

Формалізації методу мінімізації відхилення траєкторії БПЛА, під час зникнення сигналу глобальної навігаційної системи на основі фільтрації Маджвіка [1-3] (рис.1) відбувається в три етапи:

1. Етап прогнозування. На цьому етапі відбувається процес обчислення вектора кутової швидкості на основі виміру даних гіроскопа, що визначає орієнтацію БАЛА в просторі, спочатку обчислюється похідна кватерніона, що описує швидкість зміни орієнтації, в результаті добутку попереднього стану позиціювання в просторі на вектор кутової швидкості.
2. Етап корекції. На цьому кроці відбувається процес корекції навігаційних параметрів за допомогою дельта кватерніонів магнітометра та акселерометра.
3. Етап адаптивного коригування на основі показників гіроскопа. В момент динамічного руху БПЛА (серії поворотів) з високо динамічним прискоренням дані датчика акселерометра неможливо корегувати, тому застосовується адаптивний коефіцієнт коригування на основі даних гіроскопа за допомогою алгоритму градієнтного спуску Нестерова.

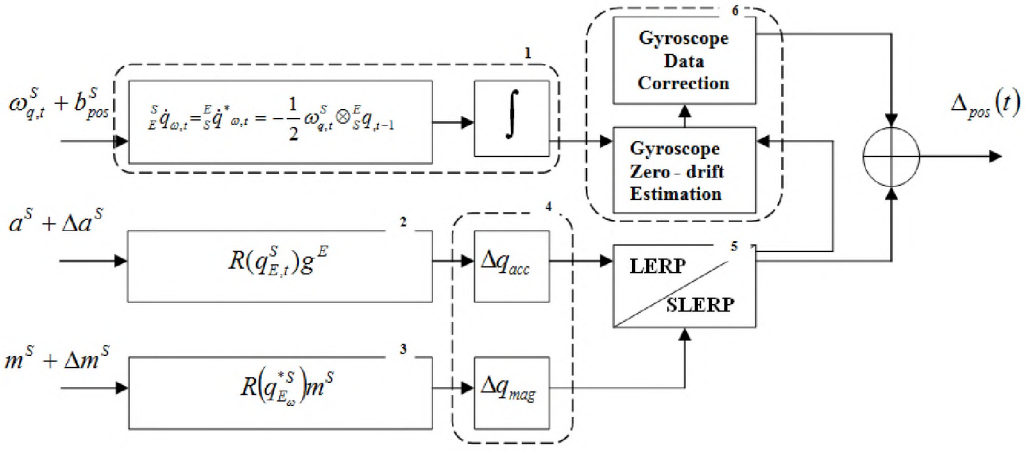


Рис. 1.Блок-схема алгоритма фільтрації МЕМС БІНС на основі вдосконаленого фільтра Маджвіка.

Опис блоків алгоритму:

Блок 1 – обробка даних гіроскопа кутової швидкості та інтегрування;
Блок 2 – обробка даних акселерометра;
Блок 3 - блок дельт кватерніонів магнітометра;
Блок 4 - фільтрація даних акселерометра та магнітометра;
Блок 5 - корекція даних акселерометра та магнітометра в кватерніонній формі;
Блок 6 – адаптивна корекція даних гіроскопа.

Експеримент проводився в програмному середовищі Matlab використовуючи реальний набір даних польоту БПЛА, на часовому інтервалі польоту БПЛА $t = \{1...300c\}$, частота дискретизації обробки навігаційних параметрів МЕМС датчиків $\Delta t = 100Hz$, швидкість БПЛА $v_{UAV} = 40km/h$.

Вихідні дані: навігаційні параметри МЕМС інерціальної навігаційної системи; m^S – показники магнітометра в локальній системі координат (відносно датчика); m^E – показники магнітометра в глобальної системі координат (відносно Землі); a^S – показники даних акселерометра (вектор порізної); $g^S_{\omega,t}$ – вектор кутової швидкості (гіроскопа); b^S_{est} –зміщення дрейфу нуля гіроскопа.

Цільова функція: $f\left(\hat{q}^S_E, \hat{a}^S, \hat{m}^S, \hat{b}^S_t\right) \to \Delta_{pos}(t) \Rightarrow \min$.

Обмеження: інші МЕМС-датчики та елементи ІНС не впливають на збільшення похибки встановлення кутової швидкості;

Допущення: $v_{UAV} = 40km/h = const$.

За результатами експеременту запропонований метод на основі вдосконаленого фільтра Маджвіка показує кращу швидкість обробки даних навігаційних параметрів та точність визначення параметрів позиціювання в просторі БПЛА на базі безплатформної інерціальної системи навігації (БІНС) мікро електромеханічної системи (МЕМС) в порівнянні з методами фільтрації на основі розширеного фільтра Калмана на 32%, та Маджвіка 20%.

Відмінність запропонованого методу, від існуючих полягає в наступному:

по перше зменшує вплив феромагнітного шуму на компоненти курсу і тангажу, коли датчик магнітометра збурений локальним феромагнітним шумом;

по друге запропонований метод не використовує складних обчислень матричних інверсій при цьому підтримує низькі обчислювальні затрати за рахунок застосування алгоритму лінійної інтерполяції;

по третє швидка збіжність кватерніона орієнтації БПЛА за рахунок алгебраїчного рішення;

по четверте два різних коефіцієнта підсилення для процесу роздільної фільтрації порізної швидкості та феромагнітних шумів магнітного поля;

по п'яте під час польоту БПЛА в динамічному середовищі застосовується алгоритм градієнтного спуску Нестерова для обчислення компоненти кватерніонної похибки орієнтації в момент часу t-1, при цьому зменшує обчислювальні затрати та час на пошук мінімуму функції похибки навігаційних параметрів БІНС МЕМС.

Напрямком подальших досліджень є розробка інтелектуальної системи управління групою БПЛА з урахуванням особливостей організації каналів управління і зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

3. Fesenko O., Bieliakov R., Radzivilov H. and oth. (2022) Method of improving the accuracy of navigation MEMS data processing of UAV inertial navigation system.National University «Zaporizhzhia Polytechnic». Radio Electronics, Computer Science, Control.The scientific journal. Published four times per year No 3(62) 2022.

4. Fesenko O., Bieliakov R., Radzivilov H. and oth. (2020) Trajectory Control Method Of UAV In Autonomous Flight Mode Using Neural Network MELM Algorithm. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). 25-27 Nov. 2020. https://doi.org/10.1109/ATIT50783.2020.9349317.

5. Фесенко О.Д.,Бєляков Р.О.,Радзівілов Г.Д. Керування БПЛА методика керування траєкторією бпла в автономному режимі польоту на основі нейромережевого алгоритму MELM–MADGWICK. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: матерXIII наук.-практ. конф. ВІТІ.3-4 грудня 2020 року. Київ: ВІТІ, 2020 С. 270.

Ph.D. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
к.т.н. Бовда Е.М. (ВІТІ ім. Героїв Крут)
Кондратюк А.Г. (ВІТІ ім. Героїв Крут)

ВЕКТОР ТРАНСФОРМАЦІЇ АНАЛІТИЧНИХ ЗУСИЛЬ СИЛ ОБОРОНИ УКРАЇНИ У ВІЙНІ ЧЕТВЕРТОГО ПОКОЛІННЯ

Нинішнє застосування збройної сили російською федерацією проти суверенітету і територіальної цілісності України доцільно характеризувати як війну четвертого покоління (Fourth generation warfare (4GW)), оскільки комплекс заходів даного соціально-політичного явища цілком відповідає основним її характеристикам:

асиметрична війна;

нелінійність тактики;

військові дії зводяться до серії операцій;

відсутність межі між фронтом і тилом, внаслідок можливості застосування дистанційних засобів знищення (досяжність авіації, ракетний обстріл);

високотехнологічність;

використання інструментів інформації та технологій із використанням кіберпростору;

зростання ролі інформації та дезінформації у досягненні цілей війни (медійна пропаганда та гібридна війна);

відсутність межі між війною та миром;

терористичний або партизанський стиль війни.

Умови 4GWобумовлюють актуальність питання вибору пріоритетів органами стратегічного управління Збройними силами та іншими військовими формуваннями держави, здатних забезпечити максимальну ефективність застосування сил оборони та безпеки України у протидії ворожій збройній агресії проти суверенітету та територіальної цілісності України.

Одним з таких пріоритетів є системне збільшення ролі інформаційних технологій (ІТ) у процесі виконання службових (бойових) завдань силами оборони та безпеки України, оскільки окрім забезпечення основного способу автоматизації їх діяльності, зокрема у процесах управління та інформаційної взаємодії, дозволяє здійснювати безпосередній контакт із ворогом без потенційної загрози життю і здоров'ю особового складу. Так, надзвичайну ефективність у ході ведення бойових дій демонструють технології розпізнавання зображень сучасних супутникових систем, інтелектуальні боєприпаси ударних оперативно-тактичних безпілотних літальних апаратів, підсистеми інерціальної (GPS) навігації систем реактивної артилерії, інформаційні системи попереднього виявлення,вітчизняні програмні рішення управління системами артилерійського вогню, численні засоби дистанційної (артилерійської) розвідки, що дозволяє значно підвищити ефективність застосування сил оборони та безпеки держави вищим керівництвом.

Поряд з цим, інтелектуальній підтримці прийняття раціональних рішень засобами ІТ у ході ведення повномасштабної війни не приділяється належної уваги, що у свою чергу нерідко призводить до факту зіткнення із ворожою агресією в умовах, які не було передбачено. Так, суб'єктивне судження численних військових експертів стосовно потенційного широкомасштабного вторгнення російської федерації в Україну було хибним, і, як наслідок у багатьох аспектах підготовкадо захисту суверенітету та територіальної цілісності почалась лише за кілька годин до наступу.

У доповіді пропонується вектор трансформації аналітичних зусиль сил оборони та безпеки держави, зокрема у аспекті інтелектуального аналізу даних про ворога із використанням алгоритмів машинного навчання та технологій штучного інтелекту (перевизначити показники інтелекту, збільшити можливості обробки та аналізу). У зв'язку із можливістю доступу до різноманітної інформації про потенційного ворога (Інтернет, засоби масової інформації (ЗМІ), розвідувальні дані) та із врахуванням багаторічної шаблонної

поведінки російської федерації у попередніх війнах: війна в Афганістані; війна в Абхазії, Придністровський конфлікт; Перша російсько-чеченська війна; Друга чеченська війна; Російсько-грузинська війна 2008 року існуючого стеку вказаних технологій цілком достатньо для обробки усієї множини можливих стратегічних дій противника, у тому числі і в кіберпросторі, що дозволило би бути готовим до будь-якого розвитку подій.

Наприклад, у ряді наукових праць доведено наявність закономірностей між викидом спеціальної інформації у ЗМІ російської федерації та перед кожною спеціальною операцією. Інший приклад – наслідок асиметричної війни – в умовах обмеження кількості озброєння вищому керівництву Збройних сил України доводиться обирати пріоритетну ціль із множини потенційних ворожих цілей для нанесення противнику максимального ураження. Так, формалізація протистояння у ході війни шляхом інтелектуальної гри дозволяє:

притримуватись постулатів класичної воєнної науки (ворога потрібно вивчати до початку війни, а не на полі бою);

забезпечувати домінування якості над кількістю (високотехнологічна зброя);

позбутися суб'єктивності судження під час прийняття рішень;

визначати неочевидний можливий наступний хід противника у ході бойових дій (ведення наступальних/контрнаступальних кібероперацій);

розширити можливості застосування найсильнішої зброї – інформації.

Варто зазначити, що на сьогоднішній день країни-партнери України значною мірою сприяють інтелектуалізації процесу прийняття рішень вищим командуванням сил оборони і безпеки нашої держави засобами Центрального розвідувального управління Сполучених Штатів Америки (англ. Central Intelligence Agency)та американського аналітичного центру – інституту вивчення війни (англ. Institute for the Study of War).За їхніми даними, уже сьогодні потрібно готуватись до війни п'ятого покоління 5GW – війни, у якій жертва навіть не усвідомлює, що вона є жертвою війни (війна, що не ідентифікується). Навідміну від попередніх війн, для 5GWбажаний результат полягає у тому, щоб впливати, а не бути видимим, зокрема засобами ІТ.

Таким чином, одним із підходів забезпечення максимальної ефективності застосування сил оборони та безпеки України у протидії ворожій збройній агресії проти суверенітету та територіальної цілісності України є застосування комп'ютерних ІТ, зокрема у аспекті інтелектуальної підтримки прийняття рішень, оскільки дозволяє у інтелектуальній грі протиборчих сторін завжди бути на крок попереду та у багатьох випадку зберегти життя і здоров'я військовослужбовців.

Ph.D. Фесьоха В.В. (ВІТІ ім. Героїв Крут)
Кисиленко Д.Ю. (ВІТІ ім. Героїв Крут)
Турчак О.Р. (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ ІСНУЮЧИХ РІШЕНЬ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Технологічна ескалація (цикл неперервних технологічних удосконалень протиборчих сторін у своїх спробах перемогти один одного)у кіберпросторі залишаєвідкритим питання ефективного забезпечення конфіденційності, доступності та цілісності даних інформаційних систем(ІС) критичної інфраструктури, зокрема ІС військового призначення.Причому досягти ситуації паритету зі сторони, яка здійснює кіберзахист у протидії кіберзлочинності (кібершпигунству) в режимі реального часунадто складно, оскільки ентропія комплексуїх заходів є максимальною.Як правило, така перевага зі стороніздійснення інформаційно-руйнівного впливу реалізується засобами нового (некласифікованого) шкідливого програмного забезпечення (ШПЗ, комп'ютерних вірусів), боротися з яким, як правило, можливоне раніше стадії ліквідації їх наслідків.

Аналіз публікацій за даною тематикою показавперевагу підходуімовірнісного аналізу (евристичний аналіз; виявлення змін; резидентні монітори) перед сигнатурним у процесі виявлення ШПЗ, оскільки у певній мірі дозволяє виявляти нові його екземпляри. Найбільшу ефективність серед існуючих демонструє метод евристичного аналізу, суть застосування якого полягає у контролі виконання програмного коду на предмет ідентифікації підозрілої (подібної до вірусної) активності у результаті чого з прийнятною точністю вдається виявляти поліморфні та метаморфні віруси (здані змінювати свою сигнатуру). Поряд з цим, основними недоліками даного класу методів є значна обчислювальна складність у процесі інспекції програмного коду та відносно велика кількість хибних спрацьовувань (нова активність легітимного програмного забезпечення ідентифікується як шкідлива).

У зв'язку з цим, виникає актуальне наукове завданнярозробки (удосконалення) нових підходів, здатних виявляти деструктивну діяльність ШПЗ із високою точністю в умовах прийнятної обчислювальної складності.

На основі викладеного, пропонується удосконалення існуючих систем антивірусного захисту шляхом реінжинірингу їх функціональної архітектури, зокрема додаванням модулів визначення вектора вірусів, та нечіткої їхідентифікації. Так, в основу функціоналу модуля визначення вектора вірусівна етапі навчання (донавчання)антивірусної системи доцільно покласти математичний апарат (клас методів кластеризації та/або зменшення досліджуваної розмірності ознак) усунення зайвої дисперсії (неінформативних) досліджуваних ознак із офіційних наборів даних про функціонування ШПЗ. Отримана у результаті множина значущих досліджуваних ознакдостатньо повно характеризує вектор впливу ШПЗ (програмного вірусу), оскільки зашифроване тіло ШПЗ у випадку використання підходу поліморфізму та змінена сигнатура програмних сміттям у випадку використання підходу метаморфізму не здатні приховати ознак їх деструктивної діяльності.У противному випадку ШПЗ змінить клас належності і буде ідентифіковано або втратить деструктивне ядро.

Наступним етапом є автоматична генерація правил для нечіткого класифікатора з метою усунення суб'єктивних експертних суджень.В основу модуля нечіткої ідентифікації ШПЗ доцільно покласти математичний апарат теорії нечіткої логіки, оскільки саме такий підхід дозволяє здійснювати ефективневиявлення деструктивного впливу ШПЗ в умовах наявності багатьох його можливих форм. Таким чином, запропоновані перспективи удосконалення існуючих рішень виявлення шкідливого програмного забезпечення в інформаційних системах військового призначення значно сприятимуть підвищенню ефективності виявлення нових зразків ШПЗ, зокрема поліморфних та метаморфних його форм особливо у поєднанні із сигнатурним підходом до їх виявлення.

Фомін М.М. (ВІТІ ім. Героїв Крут)
д.т.н. Могилевич Д.І. (ВІТІ ім. Героїв Крут)

МЕТОДИКА КОМПЛЕКСНОГО ОБҐРУНТУВАННЯ ВИМОГ ДО ЕКСПЛУАТАЦІЙНО-ТЕХНІЧНИХ ПАРАМЕТРІВ ОБЛАДНАННЯ МАРШРУТІВ ІНФОРМАЦІЙНИХ НАПРЯМКІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Високий рівень інформаційного забезпечення управлінської діяльності стає визначальним чинником досягнення переваги над противником. Досвід ведення бойових дій під час широкомасштабного вторгнення російської федерації на територію України показав домінуючу роль інформаційно-комунікаційного забезпечення системи управління військами та зброєю. Глибока зміна в техніці зв'язку і обчислювальній техніці в останні десятиліття привели до інтеграції мереж зв'язку та комп'ютерних мереж, що зробило можливим створення складних інформаційно-комунікаційних систем (мереж). На ефективність функціонування такої системи суттєво впливає надійність складових її підсистем і елементів, а також складність зв'язків між ними. Відомі в цій предметній області наукові результати присвячені в основному дослідженням різних часткових аспектів надійності і отримані, як правило, без комплексного урахування сукупності факторів, що впливають на надійність та особливості функціонування інформаційно-комунікаційних систем (мереж).

Таким чином, на теперішній час відсутня єдина методологія і ефективний науково-методичний апарат для обґрунтування вимог до експлуатаційно-технічних параметрів обладнання маршрутів інформаційних напрямків інформаційно-комунікаційних систем (мереж).

Метою дослідження є розробка методики комплексного обґрунтування вимог до експлуатаційно-технічних параметрів обладнання маршрутів інформаційних напрямків інформаційно-комунікаційних систем (мереж).

Обладнання кожної фази обслуговування маршруту інформаційно-комунікаційної системи складається з фаз обслуговування і містить певну кількість каналів зв'язку, кожний з яких має певний рівень безвідмовності та ремонтопридатності. Необхідне значення комплексного показника надійності обладнання фази можна досягти наступними шляхами: підвищенням безвідмовності, покращенням ремонтопридатності, резервуванням каналів зв'язку. На даний час розроблені методи, що дозволяють практично реалізувати кожний з зазначених вище шляхів підвищення коефіцієнта готовності при виділенні деякої суми коштів. Разом з тим, науковий і практичний інтерес представляє задача забезпечення необхідного рівня обладнання інформаційно-комунікаційної системи (мережі) при одночасному покращенні показників безвідмовності і (або) ремонтопридатності обладнання кожної фази обслуговування та використанні структурного резервування, тобто виділення резервних каналів.

Отже, потрібно вирішити задачу комплексного обґрунтування таких вимог до рівня готовності кожного каналу та кратності їхнього резервування в кожній фазі обслуговування, які б забезпечили екстремальне значення коефіцієнта готовності обладнання маршруту інформаційно-комунікаційної системи (мережі) при виділеній обмеженій сумі коштів.

Новизна представленої методики полягає в комплексному обґрунтуванні вимог до рівня готовності кожного каналу та кратності резервування каналів у кожній фазі обслуговування кожного маршруту напрямку інформаційно-комунікаційної системи (мережі), при яких коефіцієнт готовності досягає максимального значення.

Методика дозволяє оптимальним чином розподілити виділені кошти в кожній фазі обслуговування для забезпечення максимального значення коефіцієнта готовності обладнання.

Запропонована методика може бути ефективно використана для визначення рівня готовності кожного каналу і кратності їхнього резервування в маршруті інформаційно-комунікаційної системи (мережі).

Цімура Ю.В. (ВІТІ ім. Героїв Крут)
Хоменко П.В. (ВІТІ ім. Героїв Крут)
Тикинюк Д.І. (ВІТІ ім. Героїв Крут)

РЕКОМЕНДАЦІЇ ЩОДО ЗУСТРІЧНОЇ РОБОТИ РАДІОЗАСОБІВ ВИРОБНИЦТВА КОМПАНІЙ HYTERA CCL ТА MOTOROLA

На сьогоднішній день УКХ радіозв'язок в Збройних силах України організовується з використанням засобів транкінгового зв'язку компаній Motorola та Hytera CCL, що є провідними виробниками радіозасобів стандарту DMR.

В основі технології DMR лежить механізм TDMA (Time Division Multiple Access – багатостанційний доступ з тимчасовим розподілом каналів), що дозволяє розмістити два часових інтервали (незалежні логічні канали) на одній частотній несучі з сіткою частот 12,5 кГц. У рамках стандарту DMR розрізняють два режими роботи, а саме: режим прямого зв'язку (Direct mode) – симплексний зв'язок та режим зв'язку через ретранслятор (Repeater mode) із підтримкою технології двухчастотного сиплексу з дуплексним рознесенням FDD (Frequency Division Duplex), що надає можливість організувати два одночасних незалежних голосових з'єднань.

Радіостанції виробництва компанії Hytera CCL можуть зустрічно працювати з радіостанціями стандарту DMR виробництва компанії Motorola з використанням стандарту ARC-4 на каналах прямого зв'язку з довжиною ключа 40 біт. Для зустрічної роботи з ключами довжиною 256 біт для радіостанцій виробництва компанії Hytera CCL необхідно придбати та встановити відповідну ліцензію на використання стандарту шифрування AES-256 (ключ довжиною 256 біт, який наразі доступний не відповідає алгоритму AES-256).

Радіостанції різних виробників можуть працювати через ретранслятор, як виробництва компанії Hytera CCL, так і компанії Motorola. При цьому суттєвим недоліком є відсутність можливості повноцінного використання пароля доступу до ретрансляторів (ключа RAS). Увімкнений режим міграції дозволяє використовувати (або навмисно ставити на передачу) ретранслятор іншими радіостанціями (радіомережами), що працюють у цифровому режимі DMR, якщо частота передачі радіостанції відповідає частоті прийому ретранслятора.

Найбільш доцільним є використання радіостанцій та ретранслятора тільки одного виробника з повноцінним застосуванням ключа RAS (з вимкненим режимом міграції) та використання радіостанцій іншого виробника тими кореспондентами, які потребують лише каналів прямого зв'язку. При цьому зустрічна робота радіостанцій, які використовують канал ретранслятора, з радіостанціями іншого виробника, можлива на каналах прямого зв'язку з використанням сканування каналів.

Ретранслятори різних виробників неможливо об'єднати у єдину мережу (IP-Site Connect). Слід зауважити, що при використанні ретрансляторів виробництва компанії Motorola у мережі IP-Site Connect однорангові (підлеглі) ретранслятори отримують значення ключа RAS від головного ретранслятора. Тому якщо відключити ключ RAS на головному (наприклад, для забезпечення можливості роботи радіостанцій інших виробників, зокрема компанії Hytera CCL), то у налаштуваннях каналів ретранслятора радіостанцій виробництва компанії Motorola також необхідно видалити ключ RAS (якщо цього не зробити, обслуговуватися ретрансляторами радіостанції не будуть). В такому випадку, краще на ретрансляторах налаштовувати режим міграції, а не повністю відключати ключ RAS (це дозволить не змінювати існуючі налаштування ключа RAS на радіостанціях).

Враховуючи, що в Збройних силах України мережі транкінгового зв'язку побудовані з використанням різнотипних засобів (виробництва компаній Hytera CCL та Motorola), то впровадивши вищенаведені рекомендації отримуємо можливість їх об'єднання без використання додаткового (проміжного) обладнання.

Шаціло П.В. (ВІТІ ім. Героїв Крут)
Гаман О.В. (ВІТІ ім. Героїв Крут)

СЕРВІСИ ТА ТЕХНОЛОГІЇ НАУКОВОГО ПРИЗНАЧЕННЯ У СКЛАДІ ХМАРО–ОРІЄНТОВАНОГО СЕРЕДОВИЩА ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ АБО НАУКОВОЇ УСТАНОВИ, ЯКІ ЗДІЙСНЮЮТЬ ПІДГОТОВКУ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ СТУПЕНЯ ДОКТОРА ФІЛОСОФІЇ

Політичні та воєнні події за останнє десятиріччя існування незалежної, суверенної України змусили нашу країну жити в новій реальності і приймати рішення у відповідь на актуальні виклики XXI –го століття.

У цих умовах потреба модернізації підготовки здобувачів вищої освіти ступеня доктора філософії у ВВНЗ Збройних Сил України обумовлена, в першу чергу, викликами інформаційного, глобалізованого суспільства та цифровою трансформацією усіх сфер життя країни і зокрема – сфери військової освіти і науки.

Науково-дослідна діяльність потребує впровадження сучасних інноваційних підходів, засобів та технологій.

Окремим аспектом технологізації наукової та науково-технічної діяльності є відбір та систематизація засобів інформаційних технологій, що придатні для використання на кожному з етапів наукового (дисертаційного) дослідження.

З метою надання методичних рекомендацій з використання сервісів наукового призначення у складі хмари ВВНЗ або наукової установи, доцільно охарактеризувати ті із них, що знайшли поширення у практиці і класифікувати їх згідно з фазами, стадіям і етапами наукового (дисертаційного) дослідження.

Основними видами наукової діяльності є фундаментальні та прикладні наукові дослідження.

Розглядаючи основні типи культур організаційної діяльності коротко розглянемо професійний та проєктно-технологічний типи. Основною в професійному типі організаційної діяльності являється наукова діяльність, так як її результати формують єдину картину світу, загальні і окремі наукові теорії, на яких базується та чи інша професійна діяльність. Центром професійної культури організації діяльності являються наукові знання. Протягом декількох століть професійний тип культури організаційної діяльності був основним. У другій половині XX-го сторіччя визначились ряд протиріч цього типу культури організації діяльності (внутрішні протиріччя у структурі наукових знань; стрімке зростання наукових знань; технологізація засобів виробництва знань; поділ професійних галузей виробництва на безліч спеціальностей).

В результаті виникла необхідність поєднати переваги наукової (професійної) культури організації діяльності з новим типом, що дозволило би усунути вказані протиріччя. Таким типом культури організаційної діяльності, на сьогодні, являється її проєктно-технологічний тип.

Сутність культури організації діяльності проєктно-технологічного типу полягає у тому, що продуктивна діяльність людини поділяється на окремі завершені цикли, які називаються проєктами. У XX-ому столітті проєктно-технологічний тип організаційної культури діяльності виник в науковій діяльності, коли стала впроваджуватись вимога побудови наукових гіпотез і, як результат, наукове дослідження почало проєктуватись.

Так як науково-дослідницька діяльність здобувача вищої освіти ступеня доктора філософії являється продуктивною діяльністю то її мета визначається самим суб'єктом. В наслідок цього вбачання мети наукового дослідження стає достатньо складним процесом, який має свої власні стадії і етапи, методи і засоби.

Опираючись на категорії системного аналізу вбачання мети будемо називати проєктуванням дисертаційного дослідження.

Процес виконання мети дослідження характеризується:

- своїм змістом;
- своїми формами;
- специфічними методами і засобами, характерними цьому дослідженню;
- своїми технологіями.

Особливе місце серед компонентів діяльності займає саморегуляція. У випадку колективного виконання наукового дослідження необхідно включити не компонент саморегуляція, а компонент управління.

Таким чином, в структурі наукового (дисертаційного) дослідження за часом виділяють фази, стадії і етапи.

За винятком концептуальної фази наукового дослідження, фаза проєктування наукового дослідження, технологічна фаза наукового дослідження та рефлексивна фаза наукового дослідження – являються фазами проєктування і реалізації наукового дослідження.

В технологічній фазі можна виділити наступні стадії:

а) формування технології проведення наукового дослідження;

б) вибір схеми технологічної реалізації наукового дослідження;

в) реалізація програми проведення наукового дослідження;

г) перевірка справедливості сформульованої на проєктній стадії наукової гіпотези.

Однією з вимог технології наукового дослідження, яка реалізується у проєктно-технологічному типі культури організації діяльності, вона повинна враховувати, що її реалізація буде здійснюватись, як правило, в штучних системах (програмних моделях процесу наукового дослідження), створених для забезпечення реалізації потреб програми наукового дослідження. А одним з етапів стадії формування технології виконання програми наукового дослідження є вибір (розробка) засобів проведення наукового дослідження.

Таким чином, на концептуальній фазі та передпроєктній стадії фази проєктування наукового (дисертаційного) дослідження хмарні сервіси та технології можуть бути застосовані для підтримки наступних типів діяльності:

−пошук та систематизація літературних джерел;

−складання науково-бібліографічного опису публікацій;

−пошук методики, методів, інструментарію проведення дослідження;

−підготовка інструментарію.

Для цього можуть бути використані текстові, табличні редактори, засоби обробки зображень, відео, звуку а також спеціалізовані пакети прикладних програм (ППП) з метою подання текстів анкет, протоколів опитувань, демонстраційних матеріалів тощо.

На технологічній фазі починаючи з етапу «Вибір (розробка) засобів проведення наукового дослідження» можуть бути використані спеціалізовані програмні засоби статистичного аналізу, методи для визначення об'єму вибірки для проведення дослідження, засоби підтримки планування та проєктування етапів експерименту (наприклад, PASS, MATHLAB, SYSTAT).

На стадії «Реалізація програми наукового дослідження» технологічної фази наукового дослідження хмарні сервіси і технології можуть бути використані для підтримки наступних типів діяльності:

- збір фактичних даних;
- зберігання даних;
- попередня обробка даних;
- візуалізація та подання даних;
- статистичний аналіз даних.

Основні види хмарних технологій відображають можливі напрямки використання ІКТ-аутсорсингу (ІКТ – інформаційно-комунікаційні технології. Аутсорсинг (англ. outsourcing) – сервіс, що необхідний певній системі для реалізації її основної функції, який пропонує і реалізує інша система, зовнішня відносно даної) для забезпечення хмарних обчислень в інтересах здобувачів вищої освіти ступеня доктора філософії.

Таким чином потреба модернізації підготовки здобувачів вищої освіти ступеня доктора філософії у ВВНЗ та наукових установах Міністерства оборони України зумовлена викликами нового інформаційного, глобалізованого суспільства та цифровою трансформацією усіх сфер життя (зокрема освіти та науки і оборонної сфери держави)

До перспектив використання хмарних технологій у підготовці майбутніх *PhD*, варто віднести:

- розширення доступу здобувачів до кращих зразків електронних освітніх ресурсів і сервісів;
- розвиток особистості;
- потенційне отримання максимально можливих результатів застосування інформаційно-комунікаційних технологій для досягнення цілей навчання та дисертаційних досліджень.

Введення окремої навчальної дисципліни (модулів до певних навчальних дисциплін) навчальної підготовки здобувачів вищої освіти ступеня доктора філософії щодо безпосередньої роботи із хмарними технологіями та сервісами дозволить досягти запланованого результату навчання – виконувати наукові дослідження на сучасному фаховому рівні.

к.т.н. Шевченко А.С. (Quipu GmbH)
Барков Б.В. (НДЦ ІВМС ЗСУ)
Толстих В.А. (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СИСТЕМ РОЗШИРЕНОГО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРНЕТИЧНІ ЗАГРОЗИ

На сьогодні операції в кіберпросторі стали одним з видів супроводження та підтримки бойових дій завдяки яким здійснюється компрометація та виведення з ладу об`єктів та елементів критичної інфраструктури. У даній ситуації критично постає питання своєчасного виявлення та захисту від кібернетичних атак та їх окремих технік.

Для виявлення кібернетичних атак операційні центри безпеки та команди реагування на кібернетичні інциденти використовують відносно велику кількість систем та технологій таких як: SIEM, системи виявлення та реагування на кібернетичні загрози кінцевих точок (EDR – Endpoint Detection and Response), засоби захисту електронної пошти та хмарної інфраструктури, великий перелік джерел інформації для аналізу даних та інші системи. Всі ці засоби призначені для моніторингу та захисту окремих складових інформаційно-телекомунікаційної системи. На сьогоднішній час процес реагування на інциденти кібербезпеки з використанням великого стеку технологій представляє трудомісткий процес який ускладнений збором, аналізом та кореляцією інформації з різних засобів моніторингу/захисту та цілком базується на компетенції аналітика, який повинен поєднати всі наявні індикатори в єдиний ланцюжок атаки.

Розвиток систем розширеного виявлення та реагування на кібернетичні загрози (XDR – Extended Detection and Response) став агрегацією в єдину екосистему багатьох систем захисту кінцевих точок, мереж, хмарних сервісів, захисту ідентифікаційних даних, захисту пошти тощо, для виявлення, розслідування та реагування на інциденти кібербезпеки. На сьогодні немає єдиної архітектури XDR системи. В цьому напрямку ведуться роботи в рамках дослідних робіт декількох XDR альянсів.

З огляду на аналіз основних можливостей XDR систем, можна виділити основі переваги від їх застосування:

– єдина платформа для виявлення, розслідування та реагування на інциденти кібербезпеки;

– оптимізація багатьох процесів операційних центрів безпеки: збір та контекстуалізація даних про інцидент, перевірка та пошук індикаторів атак;

– можливість створення комплексних індивідуальних правил та звітів для виявлення аномалій;

– автоматизація процесу реагування на інциденти;

– видимість систем та подій на різних рівнях IT інфраструктури;

– зберігання даних про події безпеки в єдиному сховищі;

– мінімізація кількості засобів захисту та моніторингу в організації;

– зменшення кількості систем різних вендорів та спрощення ліцензійної політики;

– підвищення ефективності реагування на інциденти, повна видимість метрик реагування на інциденти та показників ефективності команди реагування на інциденти.

Подальший розвиток та провадження XDR систем є одним з основних напрямків розвитку систем захисту на найближчі роки та в умовах тенденції збільшення кібернетичних атак впровадження XDR надає можливість покращити ефективність реагування на інциденти шляхом провадження більш ефективної та комплексної системи захисту і моніторингу не збільшуючи штату операційних центрів безпеки і зменшуючи затрати на підтримку систем.

к.т.н. Шишацький А.В. (ЦДТП ОВТ)
к.т.н.Троцько О.О. (ВІТІ ім. Героїв Крут)
Мягких Г.Г. (ВІТІ ім. Героїв Крут)

МЕТОДИКА РОЗПОДІЛУ СИЛ ТА ЗАСОБІВ ЗВ'ЯЗКУ УГРУПОВАННЯ ВІЙСЬК (СИЛ) В ОПЕРАЦІЯХ

Вступ

Найбільш характерними особливостями побудови систем зв'язку спеціального призначення угруповань військ (сил) в ході ведення бойових дій (операцій) є високий ступінь апріорної невизначеності стосовно оперативної обстановки та малий обсяг вихідних даних для планування зв'язку.

За таких умов важливий правильний вибір апарату оцінки прийнятих управлінських рішень, який дозволить посадовим особам органів (пунктів) управління системою зв'язку угруповань військ (сил) бути впевненим у рішеннях, що приймаються.

Прийняття рішення на побудову системи зв'язку будь-якого рівня в ході ведення операцій (бойових дій), як правило, включає визначення мети її функціонування, вибір показників і обґрунтування критеріїв оцінки, синтез альтернативних структур і пошук раціонального варіанту розгортання системи зв'язку.

Як показує досвід організації зв'язку в операціях (в ході ведення бойових дій), рішення щодо порядку організації зв'язку, залучення сил та засобів, що необхідні для забезпечення потреб в послугах зв'язку потребує:

– наявності математичного апарату, який дозволить врахувати обсяг оперативних завдань з організації зв'язку угруповань військ (сил);

– врахування чисельного складу угруповання (споживачів послуг зв'язку) військ (сил);

– тривалості операції (ведення бойових дій), а також трудовитрати, необхідні для забезпечення потреб в послугах зв'язку угруповань військ (сил).

Метою дослідження є розробка методики розподілу сил та засобів зв'язку угруповання військ (сил) в операціях.

Виклад основного матеріалу дослідження.

Методика розподілу сил та засобів зв'язку угруповання військ (сил) в операціях складається з наступної послідовності дій.

1. Введення вихідних даних. На даному етапі визначається вихідні дані для планування зв'язку.

2. Визначення типу невизначеності про стан обстановки. На даному етапі визначається тип невизначеності про стан оперативної обстановки: повна невизначеність, часткова невизначеність та повна обізнаність.

3. Визначення необхідного складу сил та засобів зв'язку. На даному етапі визначається необхідна для організації зв'язку кількість сил та засобів зв'язку, їх вид та режими роботи.

4. Вирішення прямої та зворотної задач розподілу сил та засобів зв'язку.

5. Отримання узагальнених даних вирішення прямої та зворотної задач.

Висновки:

В дослідженні проведено розробку методики розподілу сил та засобів зв'язку угруповання військ (сил) в операціях. Новизна запропонованої методики полягає у: врахуванні типу невизначеності щодо оперативної обстановки в операційному просторі та чисельності складу угруповання (споживачів послуг зв'язку) в операціях; врахуванні при плануванні заходів з розподілу та застосування сил та засобів зв'язку тривалості ведення операції (ведення бойових дій); розрахунку трудовитрат, необхідних для забезпечення потреб у послугах зв'язку угруповань військ (сил).

к.т.н. Шкнай О.В. (НДІ ВР)
Довбенко О.В. (НДІ ВР)
Дворський М.В. (НДІ ВР)

ПРОПОЗИЦІЇ ЩОДО СТВОРЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ЗАСОБАМИ РАДІОЕЛЕКТРОННОЇ РОЗВІДКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність. Результати аналізу бойових дій внаслідок повномасштабного вторгнення рф свідчать про стрімке скорочення часу необхідного для прийняття рішень відповідними особами щодо організації та здійснення ефективної протидії сучасним зразкам озброєння та військової техніки противника. Саме оперативність прийняття обґрунтованих рішень є найважливішим завданням від якого зазвичай залежить результат ведення бойових дій. Зважаючи на зазначене, дослідження питань підвищення рівня автоматизації процесів збору/обробки інформації від різних джерел добування інформації є актуальним та своєчасним.

Постановка задачі. Сучасний стан систем підтримки прийняття рішень відзначається різноманітністю та швидкодією інформаційних засобів, які входять до неї. На даний час до даної системи входять такі автоматизовані системи (АС) управління як: АС Центру оперативного управління ("Дзвін-АС"), АС бойового управління ("Ореанда-ПС"), АС тактичної ланки управління ("Простір"), АС управління військами ("Славутич", "Кропива", "Дельта") та спеціальне програмне забезпечення ("Віраж"). Разом з тим, інформація від засобів системи радіоелектронної розвідки, крім засобів радіолокаційної розвідки, на даний час надходить до пунктів управління військами у неавтоматизованому виді. Враховуючи зазначене та сьогоденні вимоги до системи управління військами постала нагальна потреба у автоматизації процесів передачі розвідувальної інформації від зазначених засобів та, відповідно, створенні АС управління засобами радіоелектронної розвідки, яка має стати складовою частиною єдиної автоматизованої системи управління та оповіщення ЗС України.

Мета. Надання пропозицій щодо створення автоматизованої системи управління засобами радіотехнічної розвідки Збройних Сил України.

Основні положення. Основною складовою розвідувальної інформації у системі радіоелектронної розвідки є дані про об'єкти розвідки, що отримані шляхом викриття функціонування джерел радіовипромінювання засобів систем радіотехнічного забезпечення противника, а саме: бортових радіолокаційних станцій (далі – РЛС) літаків (усіх видів); РЛС зенітно-ракетних й радіотехнічних підрозділів, та РЛС артилерійської і наземної розвідки.

В доповіді представлені результати досліджень основних типів джерела радіовипромінювань, які використовуються збройними силами рф та визначено їх основні тактико-технічні характеристики за якими вони можуть бути ідентифіковані як певні об'єкти розвідки на тактичному та оперативно-стратегічному рівнях.

Визначено зміст та характер інформації, що обробляється та видається комплексом контролю радіоелектронної обстановки оперативно-стратегічного рівня ("Кольчуга"), що перебуває на озброєнні Збройних Сил України, та експериментального зразка вітчизняної станції радіотехнічної розвідки (РТР) тактичного рівня ("Вектор"), яка забезпечує оцінку радіотехнічних засобів (РТЗ) противника на полі бою до 40 км (РЛС артилерійської та наземної розвідки, РЛС зенітних ракетних комплексів, РЛС радіотехнічних військ та інші).

Враховуючи склад засобів системи радіоелектронної розвідки та різноманіття форматів передачі розвідувальної інформації розроблено низку пропозицій щодо вирішення питання їх інтеграції та сумісності, створення спільних стандартів, створення єдиної бази даних. Визначено необхідність підтримання балансу між вимогами до автономності функціонування засобів та співпраці між ними при розробці вимог до автоматизованої системи управління засобами радіоелектронної розвідки. Основна проблема стандартизації протоколів обміну розвідувальними даними полягає в тому, щоб зробити стандарти

достатньо загальними для застосування їх як у складі системи радіоелектронної розвідки, так й відповідати вимогам до функціоналу самих засобів. Проведено пошук компромісного рішення при формуванні вимог до формату протоколів обміну даними,програмного інтерфейсу (API) та програмного забезпечення (StructuredQueryLanguage (SQL), віддаленого доступу до даних (RDA), технологічного стандарту CommonObject-RequestBrokerArchitecture (CORBA)) для забезпечення можливості функціонування в CommonOperatingEnvironment (COE). Інтеграція даних від засобів системи радіоелектронної розвідки є ключовим питанням при створенні автоматизованої системи управління засобами радіоелектронної розвідки Збройних Сил України. Для вирішення питання із відмінностями у визначенні даних та їх представленні, запропоновано використати підхід, що передбачає використання посередницької бази даних. Бази даних можуть різнитися багатьма способами. Категорії гетерогенності узагальнюються нижче:

гетерогенність платформи — наприклад, відмінності в системах керування базами даних (СУБД) засобів,

гетерогенність моделі даних — наприклад, різні моделі даних, мови запитів, обмеження цілісності та схеми,

семантична гетерогенність — наприклад, конфлікти в специфікаціях даних, назвах відношень та атрибутів, рівнях точності, рівнях абстракції, одиницях вимірювання й невідповідності даних.

Враховуючи вищезазначене, до складу автоматизованої системи управління засобами радіоелектронної розвідки Збройних Сил України пропонується включити об'єктно-орієнтовану базу даних розвідувальних ознак, інтерфейс користувача, додатки для злиття треків, модельні класифікатори, детектори змін, цифровий обчислювальний комплекс, який дозволяє обробляти на високій швидкості результати просторово-часової селекції сигналів, системи обміну даними із споживачами системи.

Використання отриманих результатів дозволить сформувати загальні вимоги до автоматизованої системи управління засобами радіоелектронної розвідки Збройних Сил України із врахуванням сучасних тенденції та специфічних технологій в сфері управління інформацією.

Висновок. Враховуючи зазначене, видача інформації про об'єкти розвідки, у залежності від її призначення, до АС Центру оперативного управління ("Дзвін-АС"), АС бойового управління ("Ореанда-ПС"), АС тактичної ланки управління ("Простір"), АС управління військами ("Славутич", "Кропива", "Дельта") та до спеціального програмного забезпечення ("Віраж"), відкриє додаткові можливості з планування та прогнозування ведення бойових дій, що у свою чергу збільшить обізнаність про роботу РТЗ противника та своєчасне корегування своїх дій у залежності від змін бойової обстановки у реальному режимі часу.

Використання результатів дослідження надасть змогу сформувати тактико-технічні вимоги до перспективної автоматизованої системи управління засобами радіотехнічної розвідки Збройних Сил України. Напрямком подальших досліджень є пошук шляхів інтеграції вітчизняної системи радіоелектронної розвідки до розвідувальних систем країн НАТО.

к.т.н. Штаненко С.С. (ВІТІ ім. Героїв Крут)

ПРОЄКТУВАННЯ АДАПТИВНИХ ВБУДОВАНИХ СИСТЕМ У КОНТЕКСТІ ПІДВИЩЕННЯ ЖИВУЧОСТІ СИСТЕМИ УПРАВЛІННЯ СКЛАДНИМИ ОБ'ЄКТАМИ І ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Вбудовані системи (англ. *Embedded Systems*) представляють собою спеціалізовані мікропроцесорні системи, концепція розробки яких ґрунтується на тому, що такі системи взаємодіють з об'єктом управління або контролю, будучи вбудованими безпосередньо у пристрої, якими вони управляють [1].

На сьогоднішній день вбудовані системи широко використовуються в різних галузях діяльності таких, як: машинобудування та верстатобудування, авіація, автомобілебудування, атомна енергетика, банківська сфера, військово-промисловий комплекс, а також застосовуються як основа побудови автоматизованих систем управління, засобів автоматичного регулювання та управління технологічними процесами.

Перші вбудовані системи розроблялися в якості спеціалізованих цифрових пристроїв, основу яких складали інтегральні схеми малого та середнього ступеня інтеграції. Однак, з появою мікроконтролерної та мікропроцесорної техніки, а пізніше програмованих логічних інтегральних схем (ПЛІС), поняття вбудованої системи сильно трансформувалося. Так, якщо перші вбудовані системи представляли собою спеціалізовану структуру, яка мала у своєму складі центральний процесор, окремі інтегральні схеми контролерів периферійного обладнання, цифрових запам'ятовуючих пристроїв, то сучасні вбудовані системи реалізують вже технологію *System-on-Chip* (*SoC*) – система на кристалі [2].

Система на кристалі або *SoC* – це обчислювальна система, архітектура якої розроблена цільовим чином для розв'язання прикладної задачі (або класу задач) і реалізована у вигляді комплексу функціонально спеціалізованих апаратних і програмних компонент на базі конфігурованої мікроелектронної платформи.

На сьогоднішній день проєктування сучасних систем, що використовують технологію *System-on-Chip* засноване на застосуванні високотехнологічних САПР цифрових пристроїв, що вимагає від розробників глибоких знань не тільки цифрової схемотехніки та архітектур обчислювальних систем, але й знання методів синтезу спеціалізованих пристроїв з мікропрограмованим управлінням, знання високорівневих мов проєктування та методів контролепридатного синтезу. Тому процес проєктування сучасних вбудованих систем – це процес створення власних та використання стандартних цифрових компонентів інтелектуальної власності, які є не тільки схемотехнічним описом, але, по суті, є повноцінними проєктними документаціями з функціонального та параметричного моделювання, верифікації та виготовлення із застосуванням сучасних технологій.

Слід зазначити, що в процесі функціонування вбудованих систем можливі збої, відмови, несправності як апаратного, так і програмного забезпечення при виникненні несприятливих впливів (наприклад, іонізуючого та електромагнітного випромінювання, кібератак, шляхом застосування вірусних програм, а саме мережевих черв'яків, вірусів-маскувальників, вірусів-шпигунів, вірусів-зомбі, вірусів-блокувальників, троянських вірусів). Як наслідок таких впливів може бути порушення правильності функціонування або перехід спеціалізованої мікропроцесорної системи в непрацездатний стан, що зрештою може призвести до катастрофічних наслідків у системі управління складними об'єктами та технологічними процесами.

Так, у роботі [2] з метою підтримки мікропроцесорної системи в стані правильного функціонування внаслідок несприятливих впливів запропоновано використовувати в якості елементної бази при проєктуванні систем, які розглядаються, інтегральні схеми з програмованою структурою.

Програмовані логічні інтегральні схеми мають характерну особливість, а саме змінювати внутрішні зв'язки між логічними елементами (найпростішими логічними

функціями), що дозволяє зробити реконфігурацію внутрішньої структури мікропроцесорної системи, на відміну від програмованих мікроконтролерів і одноплатних комп'ютерів Raspberry Pi, які мають фіксовану архітектуру та фіксований набір команд. Дана особливість ПЛІС дає можливість, застосовуючи сучасне середовище розробки цифрових пристроїв, наприклад, САПР Intel Quartus Prime, проєктувати адаптивні вбудовані системи, в яких реконфігурація архітектури буде проводитися за результатами тестового або функціонального діагностування внаслідок несприятливих впливів.

Якщо розглядати адаптацію вбудованих систем до зовнішніх факторів, то вона безпосередньо пов'язана з такою властивістю складних систем як живучість, під якою розуміється здатність системи протистояти несприятливим впливам і досягати мети функціонування за рахунок зміни поведінки і структури [3]. При цьому згідно з [4] підвищення живучості здійснюється розвиненими механізмами розпізнавання, протидії та відновлення, а також спеціальними засобами реконструкції, реконфігурації та реорганізації, які представляють собою адаптивний процес.

Проєктування адаптивних вбудованих систем є досить типовою задачею проектування складних систем організаційного типу. При проєктуванні таких систем однією з основних задач є синтез структури, що визначає внутрішню організацію та відносно стійкі взаємозв'язки елементів системи. Так, згідно з агрегативно-декомпозиційного підходу під синтезом структури адаптивної вбудованої системи будемо розуміти процес послідовного вирішення системно пов'язаних задач синтезу основних елементів і частин системи. Дані задачі вирішуються ітераційно в силу їхньої взаємопов'язаності, неповноти вихідних даних та необхідності коригування отриманих рішень [5].

На першому етапі визначається організаційна структура вбудованої системи, виходячи з цілей і стратегій функціонування системи управління складними об'єктами і технологічними процесами. У результаті визначається кількість рівнів ієрархії та вузлів системи, тобто визначається топологічна структура.

На другому етапі визначається функціональна структура, тобто оптимізується розподіл функцій, які виконуються, задач за рівнями та вузлами системи з подальшим перерозподілом при виникненні несприятливих впливів.

На третьому етапі вибирається комплекс обчислювальних засобів, здатних реконфігурувати внутрішню структуру вбудованої системи на рівні елементної бази.

На останньому етапі аналізується динаміка роботи вузлів обраного варіанта структури вбудованої системи з використанням імітаційної моделі.

Таким чином, вирішення основних задач синтезу структури при проєктуванні адаптивних вбудованих систем дозволить провести реконфігурацію архітектури на рівні логічних елементів і, як наслідок, підвищити живучість не тільки мікропроцесорної системи, а і всієї системи управління складними об'єктами і технологічними процесами в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Crespo, P. Albertos, J. Simó, Embedded control systems: from design to implementation, Ifac Proceedings Volumes, Volume 40, Issue 1, 2007, Pages 25 – 32.

2. S. Shtanenko, Y. Samokhvalov, S. Toliupa, O. Silko, Increasing Survivability of Technological Systems Based on the Technology of Programmable Logic Device, Conference: Information Technology and Implementation (IT&I-2021), December 01-03, 2021, Kyiv, Ukraine At: CEUR Workshop Proceedings (Vol-3132), 2022, pp. 237 – 245.

3. Додонов А. Г. Живучесть информационных систем / А. Г. Додонов, Д. В. Ландэ. К.: Наук. думка, 2011. 256 с.

4. Додонов А.Г. Живучесть компьютерных систем и безопасность информационной инфраструктуры / А.Г. Додонов, Е.С. Горбачик, М.Г. Кузнецова // Известия Южного федерального университета. Технические науки. 2007. № 76(1). С. 203 – 207.

5. Цвиркун А.Д. Структура сложных систем. М.: Советское радио, 1975. 200 с.

Яровий В.С. (ВІТІ ім. Героїв Крут)
к.т.н. Радзівілов Г.Д. (ВІТІ ім. Героїв Крут)
д.т.н. Міночкін А.І. (ВІТІ ім. Героїв Крут)

НЕОБХІДНІСТЬ УДОСКОНАЛЕННЯ СИСТЕМИ ЕНЕРГОЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ БОЙОВОГО ЕКІПІРУВАННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ ПІДРОЗДІЛІВ ВІЙСЬКОВОЇ РОЗВІДКИ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність, постановка задачі. Головним призначенням екіпірування "солдата майбутнього" є підвищення бойової ефективності як окремо взятого бійця, так і підрозділу загалом.

Одночасно в декількох країнах світу постійно проводиться робота щодо розробки та впровадження у реальність принципово нового комплексного спорядження та озброєння рядового бійця, яке в подальшому стане цілісною бойовою системою.

На сьогодні окремі елементи цієї концепції вже стали реальністю та використовуються в Збройних Силах України та інших військових формування для вирішення поставлених завдань.

В умовах ведення війни рф проти України постійно виникають все нові і нові завдання, метою яких є зниження фізичного навантаження і підвищення мобільності бійця. Крім того, стоїть завдання підвищити життєздатність та боєздатність військовослужбовця на полі бою, оснастити його сучасними системами та підсистемами, що дадуть йому змогу максимально довго бути енергонезалежним. Особливо це стосується військовослужбовців розвідувальних підрозділів, які виконують завдання окремо від місця дислокації підрозділу протягом тривалого часу.

Мета. Метою доповіді є визначення проблем та створення системи енергозабезпечення комплексу бойового екіпірування військовослужбовців сухопутних військ Збройних Сил України.

Основні положення. В провідних країнах світу велика увага приділяється розвитку та оснащення збройних сил, починаючи від найбільш складних систем озброєння і військової техніки, закінчуючи окремим військовослужбовцем. Війна рф проти України показала, що все ж таки цієї уваги приділяється не достатньо.

Проведений аналіз показав, що провідні країни світу приділяють значну увагу комплектам бойового екіпірування військовослужбовця та не жалкують великих коштів, яких вони коштують, особливо щодо розвитку зразків засобів зв'язку, засобів розпізнавання, засобів обробки, відображення і прийому/передачі інформації, засобів орієнтування і навігації, засобів забезпечення життя та здоров'я військовослужбовця, а також їх контролю. Враховуючи бойовий досвід Україна також приділяє значну увагу виявленню та усуненню виникаючих проблем.

Беручи до уваги досвід провідних країн світу по розробці та впровадженню комплекту бойового екіпірування та власний бойовий досвід України можна виділити основні моменти щодо того, який має буди комплект бойового екіпірування військовослужбовця.

Комплект бойового екіпірування військовослужбовців, а особливо розвідників, необхідно розглядати як окрему бойову одиницю, яка повинна бути оснащена найсучаснішим обладнанням, яке б забезпечувало їм:

виконувати поставлені завдання у відриві від основних підрозділів максимально довгий період часу;

підтримувати зв'язок, приймати/передавати необхідну інформацію та її обробку;

орієнтуватися на не знайомій місцевості, а також здійснювати навігацію.

Досвід застосування розрізнених підсистеми зв'язку, розпізнавання, орієнтування і навігації, обробки і відображення інформації в зоні безпосереднього проведення бойових дій дозволяє визначити основні пріоритетні напрямки розвитку системи управління комплекту бойового екіпірування солдата, а особливо розвідника Збройних Силах України, а саме:

1. Розвиток підсистеми зв'язку.
2. Розвиток підсистеми навігації та орієнтування.
3. Розвиток підсистеми відображення та обробки інформації.
4. Розвиток підсистеми єдиного програмного забезпечення.
5. Розвиток системи енергозабезпечення.

Проведений аналіз засобів зв'язку, які використовуються або можуть використовуватися дає змогу виділити основні пріоритетні моменти перспективного складу засобів зв'язку, засобів розпізнавання, засобів обробки і відображення інформації, засобів орієнтування і навігації та елементів їх енергозабезпечення, а саме:

1. Уніфікований, автоматизований, розвід - і завадозахищений, цифровий УКХ та КХ засіб радіозв'язку.
2. Засіб відображення інформації для своєчасного отримання команд, наказів та ефективного управління боєм.
3. Засіб орієнтування та навігації для орієнтування на місцевості, отримання інформації про дружні підрозділи на карті місцевості, застосування безпечного для своїх підрозділів вогневого ураження, ефективного планування та управління солдатом на полі бою.
4. Уніфікований комплект, з відповідними перетворювачами напруги, Li-ion акумуляторів з гнучкими сонячними панелями, для його підзарядки.

Враховуючи вище зазначене науково-дослідні установи Міністерства оборони України та Збройних Сил України проводять науково-дослідні та дослідно-конструкторські роботи щодо створення таких комплектів для власних потреб, з урахуванням особливостей ведення бойових дій в умовах війни, яку розпочала рф проти України.

Таким чином система управління комплекту бойового екіпірування (СУ КБЕ) повинна складатися з підсистем:

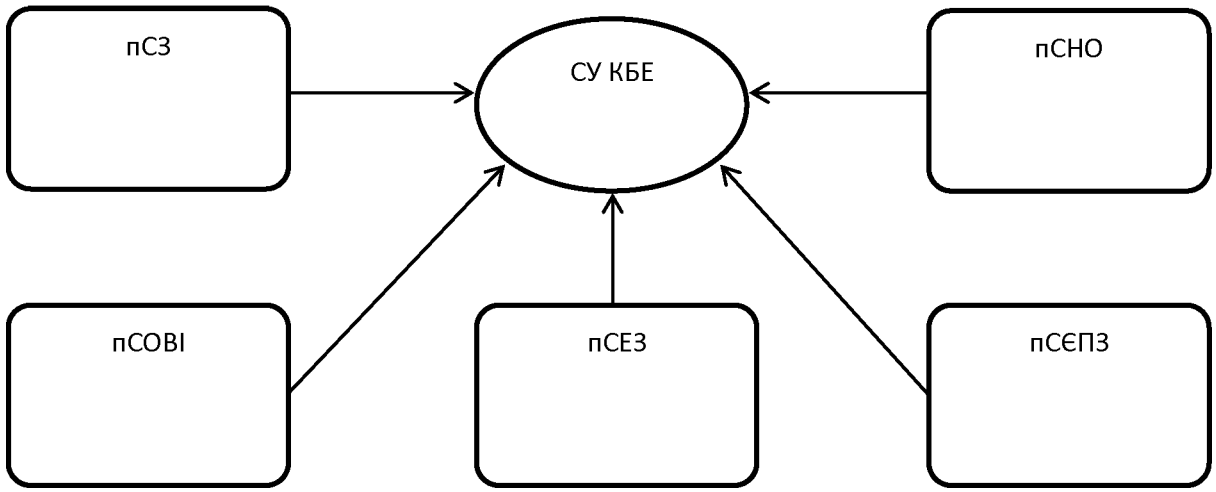


Рис. 1. Структура системи управління комплекту бойового екіпірування
підсистема зв'язку (пСЗ);
підсистема навігації та орієнтування (пСНО);
підсистема обробки і відображення інформації (пСОВІ);
підсистема єдиного програмного забезпечення (пСЄПЗ);
підсистема енергозабезпечення (пСЕЗ).

Висновки. Таким чином система енергозабезпечення комплекту бойового екіпірування пропонується наступного складу:

1. Обов'язкова наявність додаткової АКБ до індивідуальної радіостанції.
2. Комплект Li-ion акумуляторів, типу "power-bank", ємністю не менше 30000 мА/год.
3. Гнучкі сонячні панелі, захисного кольору, з можливістю здійснювати заряджання комплекту Li-ion акумуляторів.
4. Можливість зарядки обладнання від промислової електромережі і бортової мережі бойових машин.