МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

MINISTRY OF DEFENCE OF UKRAINE
Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty

Системи і технології зв'язку, інформатизації та кібербезпеки
Випуск № 1 (1)

Communication, informatization and cybersecurity systems and technologies
ISSUE № 1 (1)

У збірнику викладені статті наукових та науково-педагогічних працівників, докторантів, ад'юнктів (аспірантів), курсантів, здобувачів інституту та інших установ (організацій) за наступними науковими напрямами:

перспективи розвитку телекомунікаційних систем, комплексів та засобів спеціального призначення;

захист інформації в спеціальних інформаційно-комунікаційних системах;

стан і розвиток автоматизованих систем управління військами та зброєю;

інформаційні системи та мережі, системи підтримки прийняття рішень спеціального призначення;

бойове застосування систем зв'язку та автоматизації Збройних сил України;

теорія і практика кібербезпеки та інформаційної боротьби в комп'ютеризованих системах і мережах.

Запрошуємо до співробітництва всі зацікавлені установи та організації, які проводять наукові дослідження та науково-технічні розробки за даними напрямами.

The book containes articles of scientific and teaching staff, post graduate students, adjuncts, institute applicants and other institutions (organizations) applicants in the following fields:

prospects of telecommunications systems, development, facilities and means of special purpose;

in special information protection and communication systems;

automated systems state and development of army weapons;

information systems and networks, decision support systems for special purposes;

combat use of communications systems and automation of Armed Forces of Ukraine;

theory and practice of cyber security and information warfare in computerized systems and networks.

All interested institutions and organizations, who conduct research and development in the directions state, are invited for cooperation.

Київ – 2022 – Kyiv

УДК 621
ББК Ц4 (4Укр) 39
З – 415

Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. В. А. Романюка. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2022. № 1 (1). 97 с.

ISSN 2786-6610

Науковий профіль видання:
125 – Кібербезпека;
126 – Інформаційні системи та технології;
255 – Озброєння та військова техніка

Засновник – Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
(код за ЄДРПОУ 24978555).
Свідоцтво про державну реєстрацію видання: КВ № 25184-15124 Р від 20.07.2022.
Адреса редакції: 01011, м. Київ, вул. Князів Острозьких, 45/1. Тел. 256-22-73.
Електронна адреса: naukaviti@viti.edu.ua

Відповідальний за випуск: Гришенко Н. О.
Зам. 266. Друк. арк. 15,25.
Ум.-друк. арк.14,18. Обл.-вид. арк. 13,19. Формат паперу 60×84/8.
Тираж 100 прим. (безкоштовно).
Адреса друкарні ВІТІ імені Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

ISSN 2786-6610

З М І С Т

CONTENTS

UDC 629.7:004.94

Bieliakov R. ORCID: 0000-0001-9882-3088 (MITIT)
Hritsenok K. ORCID: 0000-0001-7202-7753 (MITIT)
Hulii V. ORCID: 0000-0002-9526-4070 (MITIT)
Kubik S. ORCID: 0000-0002-5487-3566 (MITIT)

SIMULATION OF THE SYSTEM FOR CALCULATING THE SUPPLY NEEDS OF SUBDIVISIONS WHITH OF UNMANNED AERIAL VEHICLES

Бєляков Р. О., Гриценок К. М., Гулій В. С., Кубік С. І. Моделювання системи розрахунку потреб підрозділів із забезпечення безпілотними літальними апаратами.

Досвід ведення бойових дій на сході України, а після повномасштабного вторгнення російської федерації 24 лютого 2022 року – на всій території, показав, що бойове застосування безпілотних літальних апаратів (БпЛА) може призвести не тільки до тактичних успіхів, але й оперативно-тактичних та стратегічних. Разом з тим узагальнення такого досвіду та обробка статистичних даних застосування підрозділами БпЛА постає гіперперспективним напрямком наукової діяльності. Враховуючи динамічність та швидкоплинність воєнних дій, а також потребу адаптації до умов ведення бойових дій, Збройні сили України постійно набувають спроможностей до відбиття наступу переважаючих сил агресора за рахунок комплектування підрозділів озброєнням власне вітчизняного воєнно-промислового комплексу, озброєнням, що постачається партнерами, силами волонтерів та підприємствами національної економіки, постачаючи цивільні зразки БпЛА до силових підрозділів. Таке постачання потребує узагальнення і аргументування з метою рівномірного розподілу відповідно до цільового призначення військових формувань (підрозділів). Враховуючи те, що БпЛА, що застосовуються, часто не є суто військового призначення і класифікуються за дуже широким рядом характеристичних ознак, доцільно виділити ряд принципових ознак для узагальнення досвіду. У роботі виділено чотири такі категорії: за масштабом завдань, що вирішуються; за тривалістю польоту; за радіусом дії; за типом системи керування. Авторами визначено, що ці характеристичні ознаки є визначальними для формування системи забезпечення безпілотними літальними апаратами бойових підрозділів. Відомо, що із активним застосуванням засобів радіоелектронної боротьби противника та недосконалістю технологічного виконання безпілотників, що застосовуються, мають місце затримки виконання польотних завдань, що безпосередньо або напряму можуть знижувати бойовий потенціал бойових юнітів. Метою роботи є моделювання системи розрахунку потреб підрозділів із забезпечення безпілотними літальними апаратами для формування обґрунтованого підходу до розподілу ресурсів збройних формувань різного призначення.

Ключові слова: *безпілотний літальний апарат, аеророзвідка, розвідка.*

R. Bieliakov, K. Hritsenok, V. Huliy, S. Kubik. Simulation of the system for calculating the supply needs of subdivisions with of unmanned aerial vehicle.

The experience of conducting hostilities in the east of Ukraine, and after the full-scale invasion of the russian federation on February 24, 2022 in the entire territory, showed that the combat use of unmanned aerial vehicles (UAVs) can lead not only to tactical successes, but also operational-tactical and strategic ones. At the same time, the generalization of such experience and the processing of statistical data on the use of UAV units appears as a hyper-promising direction of scientific activity. Considering the dynamism and rapidity of military actions, as well as the need to adapt to the conditions of hostilities, the Armed Forces of Ukraine are constantly acquiring the ability to repel the offensive of the overwhelming forces of the aggressor by equipping units with weapons of the domestic military-industrial complex, weapons supplied by partners, volunteer forces and enterprises of the national economy, supplying civil models of UAVs to military units. Such supply requires generalization and reasoning for the purpose of equal distribution in accordance with the purpose of military formations (units). Considering the fact that the UAVs used are often not of purely military purpose and are classified according to a very wide range of characteristic features, it is advisable to highlight a number of principle features to generalize the experience. The work distinguishes four such categories: by the scale of the tasks to be solved; by flight duration; by radius of action; by type of control system. The authors determined that these characteristic features are decisive for the formation of a system of providing combat units with unmanned aerial vehicles. It is known that with the active use of the enemy's radio-electronic warfare and the imperfection of the technological implementation of the drones used, there are delays in the performance of flight tasks, which can directly or indirectly reduce the combat potential of combat units. The purpose of the work is to model the system for calculating the needs of units for the provision of unmanned aerial vehicles for the formation of a reasonable approach to the distribution of resources of armed formations of various purposes.

Keywords: *unmanned aerial vehicle, aerial reconnaissance, reconnaissance.*

Introduction. Today, unmanned aerial vehicles (UAVs) are an integral part of any advanced army. Although UAVs are a relatively new type of weapon as they stand today, they have already proven their effectiveness and necessity. UAVs for reconnaissance, UAVs for aiming and adjusting

artillery, attack UAVs are already successfully used, it is predicted that cargo and medical UAVs will soon be used to evacuate the wounded.

Certain myths, inaccuracies, and unreliable information are always born around a rapidly developing new industry. One of the reasons for this is the lack of a generalized analysis of UAV types and their application options. In addition, the expansion of the model range of unmanned aerial vehicles requires the introduction of classification according to characteristic features. The next, no less important issue is the determination of the required number of UAVs for the successful performance of combat missions.

The purpose of the work is to develop a mathematical model for calculating the required number of UAVs in combat conditions.

Analysis of scientific works of the subject area. Modern classifications are not sufficiently complete, as they do not consider the entire array of types of UAVs that exist today, due to the dynamic development of this technology [1]. In [2], it was determined that the main components of a UAV are: an aerial platform with a special landing system, a power plant, a power source for it, a power supply system, on-board radio electronic equipment (on-board control equipment and electronic elements of the target load). On-board equipment consists of on-board computer or special processors, radio navigation system signal receiver, altimeter, gyrovertical, on-board communication and data transmission system, steering mechanisms. The works [3–5] gives a fairly complete classification based on more than 10 characteristic features. In order to achieve the goal of the work, it is necessary to highlight and reveal four of them in more detail:

1. According to the scope of tasks to be solved:

- tactical; - operational-tactical; - operational-strategic.

2. According to the duration of the flight:

- short duration; - medium duration; - long duration;

3. By radius of action:

- short radius; - small radius; - long flight range; - medium radius; - far radius.

4. By type of control system:

- remotely piloted; - remotely controlled; - automatic; - remotely controlled by the navigation system.

Quadcopters (Fig. 1) have actually supplanted all other types of UAVs in short-range reconnaissance tasks. Modern technologies make it possible to make them quite light and compact, the time of their preparation for flight is reduced to a minimum. In addition, copters are maneuverable and capable of hovering at one point, unlike aircraft-type UAVs (Fig. 2, 3), which must move constantly to maintain stable flight. Today, DJI is the most mass-produced copter in the world.

Fig. 1. Quadcopters DJI Phantom 4 Pro and DJI Matrice 300 RTK

Fig. 2. Aero Vironment RQ-20 Puma – UAV with classic aircraft scheme

Fig. 3. Athlon-Avia A1-SM "Fury" - built according to the scheme of a flying wing

Among the disadvantages of copters are a short flight range compared to the aircraft type, a higher noise level, and low autonomy. At this stage of technology development, the flight range of most compact models of copters does not exceed 10 km. Larger models, carrying a large payload, rarely cross the 20-30 km range. Low autonomy refers to the dependence of the automatic flight of copters on the presence of a GPS signal. Modern models for the most part cannot perform autonomous flight only by internal sensors; therefore, in combat conditions (under the conditions of the enemy's electronic warfare means) they are used mostly in manual (semi-automatic) mode.

Aircraft-type UAVs are mostly used at distances of hundreds and thousands of kilometers. In addition, today a large number of winged UAVs use liquid fuel as an energy carrier, while the vast majority of copters are electric.

VTOL (Vertical Take-off and Landing) UAVs are created in order to combine the advantages of aircraft and helicopter types – vertical takeoff and landing with a long flight range. Theoretically, it also allows reducing the time of preparation of the complex due to the absence of means for launching. However, a combination of advantages is impossible without a combination of disadvantages. As a rule, the engines used for takeoff are not used in cruise mode, that is, they actually take the mass of the payload in the aircraft version. In addition, they create additional resistance, which negatively affects the flight range. Thus, the advantages of VTOL are fully used only where there is not enough space for take-off "like an airplane" and at the same time a long flight range is required. In other cases, it is more appropriate to use conventional schemes.

Fig. 4. VTOL UAV Lockheed-Martin "Stalker VXE30"

Fig. 5. UAV Bayraktar TB2

Thus, taking into account the peculiarities of the structure, purpose of UAVs, and the constant expansion of the model range of the presented means, the task of calculating the necessary number of UAVs for the purpose of successfully conducting combat operations of a specific unit arises, which is not covered in open sources and formally described in doctrinal and other departmental guidance documents.

In addition, the analysis of the experience of conducting hostilities shows that the need to provide UAVs for combat units in the conditions of the dynamics and rapidity of armed confrontation is constantly growing.

Presenting main material.

Today, the scope of application of UAVs is constantly expanding, in particular in the areas of aerial reconnaissance and reconnaissance and/or fire damage to the enemy. They are gradually replacing the need for traditional correctors, and this issue is particularly acute in certain units up to and including a mechanized battalion (artillery division), during operations in densely populated areas of the area, when miscalculation of fire damage can cost the lives of civilians, which is unacceptable.

The process of using a specific number of unmanned aerial vehicles for the purpose of aerial reconnaissance requires reasoning based on the types and scope of tasks and the characteristics of the UAVs themselves.

To model the system for calculating the needs of units for the supply of unmanned aerial vehicles, we will use systems of mass service with failures, since they most fully describe all possible cases in the conditions of military operations.

In order to formalize the process of providing needs for the use of unmanned aerial vehicles, it is necessary to define the initial data.

Initial data:

The link of the unit is tactical j_1, operative-tactical j_2, strategic j_3;

Depending on the method of conducting the battle (defense, offensive), the actual size of the application area of the unit with the total area will change S_A, m^2 (position, area, operational zone);

Conditional initial number of drones d of the j-th type;

Flight resource of the unit of the j-th type, H_0, flights;

The average flight mission time will vary depending on the type of UAV missions assigned to the unit of the j-th type (reconnaissance, shock, relay), T_0, sec;

The number of personnel (engineering and technical or flight personnel) participating in the maintenance and control of UAVs.

Limitation: Detachment of personnel to resume maintenance and control of the UAV is unacceptable, and does not affect the unit's combat readiness ratio;

Assumption: The total number of UAVs is limited by the staff of the j-th type unit and cannot be instantly increased or restored.

The technical condition of unmanned aerial vehicles is changing exponentially.

The aim of the research consists in finding the required number d of unmanned aerial vehicles for specific application conditions without reducing the unit's combat readiness ratio.

In the case of conducting aerial reconnaissance by several UAVs, the time for completing one flight task is

$$T_0 = T_p/d \ , \tag{1}$$

where T_p – the average time of completing one flight task, d – total number of UAVs.

In many cases T_p can be roughly defined as the eccentricity of the graph of the observation area (site area), or as the flight time from the area of concentration to the conditional center of this section.

Intensity of flying tasks

$$\mu_p = 1/T_0. \tag{2}$$

The UAV usage rate (the total number of UAVs in the unit) can be determined from the expression

$$\rho_p = \lambda/\mu \ , \tag{3}$$

where λ – the intensity of needs (applications) for reconnaissance/pre-reconnaissance for the entire unit.

In this system, there should be a sufficient number of free UAVs to meet the needs of all fire units, since waiting for a free UAV often leads to a loss of fire superiority on the battlefield and, as a result, to a decrease in the combat potential of its troops (forces).

The probability of such a situation is [14]

$$p = \frac{\rho_p}{d!}\left[\frac{1}{1+\rho+\frac{1}{2!}\rho^2+\cdots+1\frac{1}{d!}\rho^d}\right]. \tag{4}$$

Let's assume that for a certain unit of time for the execution of reconnaissance/pre-reconnaissance tasks, the combat potential will be reduced by L. Also, the operation of one UAV per unit of time leads to a decrease in the resource of the unit – K.

Below the K it is necessary to understand not only operational costs, but also the involvement of personnel (operators) to perform flight tasks for one UAV. The reduction of the flight resource during the operation of all UAVs will be K_d.

Let the failure during the performance of one flight task cause a direct decrease in the combat potential by L_0.

Then the average reduction in combat potential associated with exploitation d UAV and with number of tasks of using UAVs per time T_p and the reduction of combat potential in connection with failures per unit of time $LT_p\lambda$, on average are

$$H = L_0\lambda_p + LT_p\lambda + K_d. \tag{5}$$

In (5) T_p – average time of the average time of completing one flight task, and together with it $LT_p\lambda$ decrease as the number of UAVs in the unit increases d.

But K_d in the same conditions also increases.

Thus, the main feature of calculating the needs of units for the provision of unmanned aerial vehicles UAVs consists in choosing such a value d, in which the criterion of reducing combat potential H will be minimal, that is, that the costs associated with the involvement of personnel and the operation of UAVs and the unproductive maintenance of an excessive number of UAVs and crews (flight crew) will be the least [15].

An important indicator is the average flight task delay time T_F, which is most often associated with the technical delay required to launch the UAV (in particular, the time for landing and take-off) and T_{F_R} – delay associated with the targeted impact of the enemy's radio-electronic warfare during the flight itself.

The sum of the average delay times T_F and performing a flight task (depending on the tasks – aerial reconnaissance or fire damage) T_{FM} is equal to the average time of use of the UAV by the unit

$$T_{SFM} = T_F + T_{F_R} + T_{FM}. \quad (6)$$

Let's establish a relationship between the average number of needs to use the UAV located in the unit and the average time of the flight task. Since for a unit of time in the unit there is a need for execution λ flight tasks, and the average time of the average time of the use of UAVs by the unit – T_{SFM}, then the total duration of use of UAVs by fire units per unit of time is equal to λT_{SFM}. Since in the unit during the conduct of hostilities there may be an average of *A* requests for the use of UAVs, this value is equal to

$$A = \lambda T_{SFM}. \quad (7)$$

Similarly, the average number of requests for flight tasks for units awaiting execution will be

$$A_S = \lambda T_3. \quad (8)$$

Due to the expenditure of additional resources to reduce the delay time due to the modernization of the fleet of UAVs involved, reduce T_{F_R}, and it is possible to significantly reduce the average time of the flight task T_{FM}. At the same time, the value will also decrease T_{SFM}.

In this case, the criterion for finding the optimal number of UAVs in the unit H the specified additional costs should also be entered.

An indicator of quality

$$K_Q = \lambda\mu/d. \quad (9)$$

UAV utilization ratio (which is the main indicator for predicting the operational load during maintenance and repair by service personnel - operators, especially with a large number of UAVs)

$$K_{QUAV} = A_0/d, \quad (10)$$

where $A_0 = A - A_S$ – the average number of UAV use cases served by the available UAV fleet.

Thus, in its essence, the use of the proposed model is carried out due to the processing of statistical data of the real use of unmanned aerial vehicles with the indication of a specific type of tasks, taking into account the technological capabilities of the UAVs themselves, which is why it becomes possible to calculate their average required number in a specific link (tactical, operational tactical, operational-strategic), which corresponds to the purpose of the study.

Conclusions. Thus, the work considers the classification of existing types of UAVs to determine the defining characteristic features for determining their required number. An analysis of factors that can influence the processes of execution of combat tasks by units was carried out. It was determined that delays in the performance of aerial reconnaissance, reconnaissance, and UAV fire damage tasks can directly reduce the combat potential of units.

The main difficulty in the practical implementation of the model for calculating the needs of units for providing unmanned aerial vehicles is the use of such drones according to the principle of their availability.

The main advantage of using the proposed model it is possible to justify the needs based on the criterion of reducing the combat potential of the combat unit, which in the future provides an opportunity to evenly distribute UAV resources during the planning of fire damage to the enemy.

The direction of further research the collection and generalization of statistical data on the use of UAVs and the approbation of this model using simulation modeling should be considered.

REFERENCES

1. Carpov V. The experience of using reconnaissance UAVs in the armed conflict on the territory of Chechnya // Proceedings of the University. 2009. № 2 (92). S. 56–59.

2. On the approval of the Rules for the execution of flights by unmanned aviation complexes of the state aviation of Ukraine: [Order of the Ministry of Defense of Ukraine dated 08.12.2016 No. 661] / Information of the Verkhovna Rada of Ukraine. Document z0031-17, valid, current edition – Edition dated February 11, 2020, basis - z0095-20.

3. Military aviation equipment. Unmanned aerial vehicles. Basic terms, definitions and classification: DSTU V 7371:2013: [Order № 1010 dated 22.08.2013] / Ministry of Economic Development and Trade of Ukraine. K., 2014. S. 2.

4. Tymochko O. I. Classification of unmanned aerial vehicles / O. I. Tymochko, D. Yu. Holubnychiy, V. F. Tretiak, I. V. Ruban // Weapon systems and military equipment. 2007. 1 (9). S. 61.

5. Rogatyuk A. A. Implementation of recognition, detection and identification information technology in the form of a video data processing application / A. A. Rogatyuk // Bulletin of the Khmelnytskyi National University. 2015. № 5. S. 237–242.

6. Kutoviy O. P. Trends in the development of unmanned aerial vehicles / O. P. Kutoviy // Science and weapons. 2014. № 4. S. 39–47.

7. Dementiev D. O. Combat Aviation complexes as part of a single information-reconnaissance-navigation-strike system / D. O. Dementiev // Collection of scientific works of Taras Shevchenko KNU Military Institute. K.: MIKNU, 2015. № 27. S. 74–77.

8. Unmanned aerial vehicle «R-400» [Electronic resource]. – Access mode: http://eizvestia.com/armiya/full/386-bespilotnyj-letatelnyj-apparat-r-400.

9. Luckiy M. H. Development of international regulation and regulatory framework for the use of unmanned aerial vehicles / M. H. Luckiy, V. P. Kharchenko, D. O. Buhaiko // Collection NAU. 2015. № 4. S. 5–14.

10. Moiseev V. S. Applied theory of control of unmanned aerial vehicles: monograph / V. S. Moiseev. Kazan: HBU "Republican Center for Monitoring the Quality of Education" (Series "Modern Applied Mathematics and Informatics"), 2013. S. 768.

11. Rostopchin V. V. Unmanned aircraft systems: basic concepts / V. V. Rostopchin, I. Ye. Burdun / Electronics: Science, Technology, Business. 2016. № 7. S. 82–88.

12. Salnik Yu. P. Analysis of the technical characteristics and capabilities of unmanned aerial systems of operational-tactical and tactical radius of action of the armies of developed countries / Yu. P. Salnik, I. V. Matala // Military and technical collection. 2013. № 7. S. 70–74.

13. Unmanned flying taxi Ehang 184 is already being tested in the skies over Dubai [Electronic resource]. Access mode: https://itc.ua/blogs/bespilotnoe-letayushhee-taksi-ehang-184-uzhe-testiruyut-v-nebe-nad-dubaem-video.

14. Kharchenko O. V. Classification and trends in the creation of unmanned aerial vehicles for military purposes / O. V. Kharchenko, V. V. Kulescin, Yu. V. Kocurenko // Science and defense. 2015. № 6. S. 47–54.

15. Priymak A. V. Analysis of the feasibility of creating and using multifunctional unmanned civil aviation complexes / A. V. Priymak, Ya. V. Daryin, D. M. Stryuk, A. A. Slobodianuk // Weapon systems and military equipment. 2010. № 3 (23). S. 142–145.

16. Takha Kh. Introduction to operations research / Kh. Takha. M.: «Vil'yams», 2001. 912 s.

УДК 621.391.372

Бондаренко Л. О. ORCID: 0000-0003-1850-0508 (ВІТІ)
Руденко В. І. ORCID: 0000-0003-3563-5486 (ВІТІ)
Ченченко В. А. ORCID: 0000-0003-1369-4075 (ВІТІ)
Плугова О. Б. ORCID: 0000-0001-7848-7806 (ВІТІ)

ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ РАДІОЛІНІЙ З ПСЕВДОВИПАДКОВОЮ ПЕРЕБУДОВОЮ РОБОЧОЇ ЧАСТОТИ

Необхідність постійного вдосконалення засобів радіозв'язку випливає зі зростаючої потреби передачі голосу і даних з високою живучістю і пропускною спроможністю каналів в радіолініях, що забезпечують обмін інформацією між органами військового управління, підрозділами, системами озброєнь і окремими військовослужбовцями.

Радіостанції можуть працювати як на фіксованій частоті, так і у режимі псевдовипадкової перебудови робочої частоти (ППРЧ). За відсутності організованих радіозавад встановлюється режим роботи радіолінії на фіксованій частоті. При використанні противником радіоелектронного придушення (РЕП), а також у разі складної завадової обстановки основним засобом захисту від придушення каналу зв'язку є ППРЧ.

Технічна реалізація режиму ППРЧ є досить складним і затратним процесом, тому його вибір може бути обумовлений лише підвищеними вимогами до завадозахисту. Крім того, системи з ППРЧ не дозволяють досягати високої швидкості передачі даних через ряд труднощів, пов'язаних із синтезаторами когерентних частот.

Ефективність систем радіозв'язку (СРЗ) визначається безліччю різних за своєю природою факторів, які умовно можна розділити на три групи: якість СРЗ, умови функціонування СРЗ, способи використання (застосування) СРЗ.

Характерними особливостями створення, розгортання та експлуатації систем радіозв'язку тактичної ланки управління є високий ступінь невизначеності характеристик їх функціонування в динаміці збройного конфлікту, що викликає необхідність постійного вдосконалення підходів до обґрунтування вибору напрямків розвитку СРЗ.

Аналіз заходів захисту від завад за допомогою введення в радіостанцію режиму ППРЧ диктує необхідність раціонального вибору часових характеристик процесу аналого-цифрового перетворення сигналів (мови і даних) і процесу пакетування перетвореної інформації в пакети з паузами, необхідними для перебудови робочої частоти каналу.

В статті відображені погляди авторів та запропоновані пропозиції до підходу обґрунтування ефективності СРЗ з ППРЧ за узагальненим показником ймовірності своєчасної та достовірної доставки повідомлень (надання послуг), який дасть можливість встановлювати вимоги до критеріїв технічних характеристик СРЗ.

Ключові слова: *ефективність, узагальнений показник, групи критеріїв, завадозахищеність СРЗ.*

L. Bondarenko, V. Rudenko, V. Chenchenko, O. Pluhova. Estimation of efficiency of functioning of radio lines with frequency-hopping spread spectrum.

The need for constant improvement of radio communications arises from the growing need for voice and data transmission with high survivability and bandwidth of channels in radio links, providing information exchange between military command and control bodies, units, weapons systems and individual military personnel.

The radio stations can operate both at a fixed frequency and in the frequency-hopping spread spectrum (FHSS). In the absence of organized radio interference, the mode of operation of the radio link at a fixed frequency is established. When using electronic suppression (ES) by the enemy, as well as in a complex jamming environment, the main means of protection against suppression of the communication FHSS.

The technical implementation of the FHSS mode is a rather complex and costly process, so its choice can be due only to the increased requirements for noise protection. In addition, FHSS systems do not allow high data rates to be achieved due to a number of difficulties associated with coherent frequency synthesizers.

The effectiveness of radio communication systems (RCS) is determined by many factors of different nature, it can be conditionally divided into three groups: the quality of the RCS, the conditions for the operation of the SRZ, the ways of using (using) the RCS.

The characteristic features of the creation, deployment and operation of radio communication systems at the tactical level of control are a high degree of uncertainty in the characteristics of their functioning in the dynamics of an armed conflict, which necessitates constant improvement of approaches to justifying the choice of directions for the development of RCS.

Analysis of noise protection measures by introducing FHSS mode into the radio station dictates the need for rational choice of time characteristics of the process of analog-to-digital conversion of signals (speech and data) and the process of packing the converted information into packets with pauses needed to adjust the operating frequency.

The article reflects the views of the authors and proposes proposals for the approach to justify the effectiveness of RCS with FHSS on a generalized indicator of the probability of timely and reliable delivery of messages (services), which will set requirements for the criteria of technical characteristics of RCS.

Keywords: *efficiency, generalized indicator, groups of criteria, noise protection of RCS.*

Постановка завдання в загальному вигляді

При створенні СРЗ для організації інформаційного обміну між територіально рознесеними об'єктами важливе місце займають питання, які визначаються характеристиками військового зв'язку – своєчасністю, достовірністю та безпечністю інформаційного обміну.

Для визначення критеріїв оцінки ефективності СРЗ необхідно встановити залежність між характеристиками СРЗ і ступенем їх впливу на бойову ефективність.

Показники оцінки ефективності СРЗ можливо розділити на дві групи: технічні та оперативно-тактичні [2].

Технічні показники дозволяють оцінювати якість характеристик інтерфейсів (радіо і канальних) за здатністю досягнення граничних якісних показників функціонування СРЗ.

Оперативно-тактичні показники є вихідними при розробці принципів функціонування СРЗ. Вони дозволяють оцінювати якість СРЗ в бою (операції).

Виходячи з цього, випливає, що рішення вище зазначених питань пов'язано зі створенням методології оцінки ефективності СРЗ, яка містить:

єдину систему показників ефективності систем і засобів військового зв'язку;

уніфіковані принципи розробки та подання нормативних моделей протиборства СРЗ і систем РЕП;

сукупність методів оцінки показників ефективності систем і засобів військового зв'язку;

способи і алгоритми розрахунку показників ефективності різних СРЗ.

Актуальність викладеного матеріалу полягає в тому, що застарілі галузеві стандарти і загальні тактико-технічні вимоги до систем і засобів військового зв'язку, де містяться основні методичні положення, терміни, поняття та визначення в галузі оцінки ефективності СРЗ, не відображають сучасну систему показників і методи їх оцінки. Це не дозволяє порівнювати між собою не тільки різні сучасні СРЗ, але і проводити їх об'єктивну оцінку на всіх етапах життєвого циклу (дослідження, розробка, виробництво, експлуатація). Крім того, немає єдиного підходу до оцінки ефективності СРЗ користувачами і розробниками.

Аналіз останніх публікацій

Метод розширення спектру радіосигналів на основі ППРЧ є достатньо вивченим і відображеним у науковій літературі. Аналіз опублікованих робіт показує, що більша частина досліджень присвячена вирішенню окремих завдань щодо вдосконалення технічних характеристик СРЗ, в яких викладаються:

основні принципи і характеристики методу розширення спектра сигналів за рахунок псевдовипадкової перебудови робочої частоти, наприклад [3–5];

аналіз можливих способів підвищення завадозахищеності типових СРЗ з ППРЧ в умовах організованих завад і власних шумів СРЗ, наприклад [6–9];

вирішуються завдання синтезу та аналізу завадостійкості адаптивних алгоритмів демодуляції сигналів з ППРЧ і частотним рознесенням інформаційних символів в умовах апріорної невизначеності щодо параметрів завади [10–14].

У роботах [15–21] запропоновані напрямки підвищення завадозахищеності СРЗ з ППРЧ та запропонована методика вибору робочих частот з урахуванням стратегій застосування засобів РЕБ та електромагнітної сумісності засобів радіозв'язку, що розгортаються в локальних угрупованнях радіозасобів.

У роботі [22] запропоновано методику вибору необхідної ширини хопсету, при якій забезпечується задана якість передачі інформації.

В монографіях [23–25] розглянуто використання ППРЧ для підвищення завадозахищеності систем радіозв'язку в умовах радіоелектронного протиборства, наведена загальна характеристика СРЗ з ППРЧ, окремо описані питання завадозахищеності сигналів з ППРЧ.

В останніх публікаціях пропонуються нові та покращені методики оптимізації (ускладнення алгоритму) формування сигналу ППРЧ, виходячи з аналізу можливої завадової обстановки в радіоканалі та характеристик методів ППРЧ.

Так, у роботі [26] запропоновано метод автоматичного визначення тривалості частотних елементів радіосигналу з ППРЧ за умов наявності вузькосмугових завад у частотному діапазоні роботи радіозасобів.

У роботах [26–28] розроблені методології формування сигналу ППРЧ при передачі голосу (мови). Сутність методології [28] полягає у розосередженні у часі сусідніх символів інформаційного сигналу, що потрапляють під вплив завади. У такому розташуванні символів мовних кадрів на інтервалі частотних елементів сигналу з ППРЧ завада вражає найменш важливі, для відтворення мови, символи.

Наукові розробки щодо підвищення завадозахищеності СРЗ з ППРЧ можуть бути використаними при розробці вітчизняних радіозасобів з ППРЧ.

Разом з тим, викладені в зазначених роботах теоретичні основи прогнозування завадової обстановки в радіоканалі, пропозиції щодо покращення алгоритмів формування сигналів з ППРЧ в умовах радіопротидії противника не враховують специфічні вимоги до систем військового радіозв'язку – оперативно-тактичні вимоги.

Мета статті. Метою даної статті є розробка пропозицій до підходу обґрунтування ефективності СРЗ з ППРЧ за узагальненим показником ймовірності своєчасної та достовірної доставки повідомлень (надання послуг), який дасть можливість встановлювати вимоги до критеріїв технічних характеристик СРЗ, які, в свою чергу, дозволять оцінювати якість характеристик інтерфейсів (радіо і канальних) по здатності досягнення граничних якісних показників функціонування систем радіозв'язку з ППРЧ.

Виклад основного матеріалу

СРЗ створюється для передачі інформації між органами військового управління, пунктами управління, системами озброєнь, окремими військовослужбовцями і служить активним засобом в їх цілеспрямованій діяльності.

В процесі застосування СРЗ постійно виникають проблеми різної складності. Причиною виникнення проблем є розбіжність між бажаним і дійсним результатом функціонування СРЗ в реальних умовах при невідомих шляхах подолання цієї розбіжності (невідповідності). Для вирішення проблеми необхідно виділити і досить чітко сформулювати цілі діяльності, здійснення яких істотно знижує або усуває відмінність між бажаним і дійсним результатом, тобто вирішити проблему.

Глобальна мета, за яку приймемо якість функціонування СРЗ, допускає декомпозицію, в результаті якої формуються взаємопов'язані цілі, які в загальному випадку можуть бути піддані подальшому поділу на більш прості складові (підцілі, завдання).

Під ефективністю функціонування радіоліній з ППРЧ будемо розуміти властивість системи досягати поставленої мети в заданих умовах з певною якістю [1; 2].

Показник ефективності повинен бути узагальнюючим показником оптимальності функціонування системи і повинен задовольняти наступним вимогам:

відображати цільове призначення системи, що досліджується;

бути пов'язаним із показниками системи вищого рівня;

мати чіткий фізичний сенс;

бути критичним до змін параметрів системи, що досліджується, і параметрів обстановки.

Основною вимогою при виборі показника ефективності є відповідність показника мети операції, яка відображається необхідним результатом. Для опису відповідності реального результату операції необхідному формально введемо числову функцію на безліч результатів операції – функцію відповідності [2].

За узагальнений показник ефективності функціонування радіолінії з ППРЧ приймемо спільну ймовірність своєчасної та достовірної доставки повідомлень (надання послуг) [1].

Найбільш повною характеристикою своєчасності доставки повідомлень по лініях радіозв'язку з ППРЧ, що характеризує їх оперативну ефективність, є інтегральна функція розподілу часу передачі повідомлень з достовірністю, не гірше заданої:

$$F(t) = P\left\{\frac{T_{\text{пер}} \le t}{D \le D_{\text{доп}}}\right\} \tag{1}$$

Під характеристикою своєчасності передачі повідомлень по воєнним лініям зв'язку розуміється ймовірність того, що час передачі повідомлення заданого обсягу $T_{\text{пер}}$ не перевищить деякого значення t при забезпеченні допустимих втрат за достовірністю. При передачі дискретних повідомлень показником достовірності зазвичай служить допустима ймовірність помилки на біт інформації.

Для побудови інтегральної функції розподілу часу передачі повідомлення в радіолінії з ППРЧ введемо такі припущення:

1. Всі частоти m, що виділені для зв'язку, є статистично однорідними, тобто ймовірності зв'язку на кожній з них з достовірністю гірше заданої рівні між собою:

$$P_{\text{зв1}}\left(D \le D_{\text{доп}}\right) = P_{\text{зв2}}\left(D \le D_{\text{доп}}\right) = \cdots = P_{\text{зв}m}\left(D \le D_{\text{доп}}\right). \tag{2}$$

При цьому значення $P_{\text{зв1}}\left(D \le D_{\text{доп}}\right)$, виходячи з (2), визначаються наступним чином:

$$P_{\text{зв1}}\left(D \le D_{\text{доп}}\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\xi} \left\{-\frac{t^2}{2}\right\} dt\,, \tag{3}$$

де D – показник достовірності;

$P_{\text{зв}}$ – ймовірності зв'язку на кожній з частот з достовірністю не гірше заданої;

$\xi = \dfrac{\bar{z} - z_{\text{доп}}}{\sigma_z}$ – розрахунковий параметр;

$z_{\text{доп}}$ – допустиме перевищення сигналу над рівнем завад.

2. Будемо вважати, що під час впливу організованих завад в смузі робочих частот радіолінії m^* частот з m будуть непридатні для зв'язку, тобто для них умова $z \ge z_{\text{доп}}$ не виконується. Дана умова може мати місце при постановці широкосмугових загороджувальних завад.

Очевидно, що час достовірної передачі повідомлення $\left(T_{\text{пер}}\right)$ визначається сумарним часом передачі повідомлення $T_{\text{с}}$, часом повторної передачі команд запитів $\left(T_{\text{кз}}\right)$ та часом повторної передачі повідомлення $\left(T_{\text{пп}}\right)$ і визначається математичним виразом:

$$T_{\text{пер}} = T_{\text{с}} + T_{\text{кз}} + T_{\text{пп}} = \sum\nolimits_{\kappa=0}^{\kappa} \left(T_{\text{кз}_\kappa} + T_{\text{с}_\kappa}\right), \tag{4}$$

де κ – кількість переданих повідомлень.

Якщо $T_{\text{кз}} \langle\langle T_{\text{с}}$, то вираз (4) можна представити у вигляді:

$$T_{\text{пер}} = \sum\nolimits_{\kappa=0}^{\kappa} T_{\text{с}_\kappa}\,. \tag{5}$$

У загальному випадку величина κ є випадковою, тому час передачі повідомлення $T_{\text{пер}}$ також є випадковою величиною. При цьому функція розподілу випадкових величин залежить не тільки від умов роботи радіолінії, а й від алгоритму її функціонування.

Так, наприклад, у відомих алгоритмах роботи радіоліній з ППРЧ не проводиться аналіз робочих частот на придатність. У цьому випадку інтегральну функцію розподілу часу передачі повідомлення для таких радіоліній можна записати в наступному вигляді [2]:

$$F(t)=\sum_{\kappa=0}^{\kappa-1}P_{\text{с}}(\kappa)U(t-\kappa T_{\text{с}})=\sum_{\kappa=0}^{\kappa-1}\left\{\ 1-\left[\left(1-\frac{m^*}{m}\right)P_{\text{зв}}\right]^{\text{N}}\ \right\}^{\kappa}\times\left[\left(1-\frac{m*}{m}\right)P_{\text{зв}}U(t-\kappa T_{\text{с}})\right]^{\text{N}},\qquad(6)$$

де $P_{\text{с}}(\kappa)$ – ймовірність передачі повідомлення після κ повторень;

$\left(1-\frac{m^*}{m}\right)$ – ймовірність того, що чергова частота не буде схильна до впливу організованої завади;

$P_{\text{зв}}$ – ймовірність зв'язку на частоті;

$U(t-\kappa T_c)=\begin{cases}1, \textit{ при } t\geq \kappa T_{\text{с}}\\ 0, \textit{ при } t<\kappa T_{\text{с}}\end{cases}$ – функція ймовірності випадкової події.

За допомогою виразу (6) можна оцінювати оперативну ефективність радіоліній з ППРЧ без використання додаткових заходів підвищення достовірності прийому сигналів, які здійснюють передачу цифрових повідомлень, залежно від умов поширення радіохвиль $(P_{\text{зв}})$ і завадової обстановки (m^*) на виділеній групі частот, а також з урахуванням найважливіших характеристик режиму ППРЧ – швидкості ППРЧ $(V_{\text{ППРЧ}})$ і кількості виділених частот (m).

Результати розрахунків за формулою (6) у вигляді графіків представлені на рис. 1.

Аналіз розрахунків дозволяє зробити наступні висновки:

радіолінії з ППРЧ без додаткових заходів підвищення достовірності мають низьку ефективність. Так, наприклад, ймовірність одноразової передачі повідомлення тривалістю $T_{\text{с}}$ = 0,1с (повідомлення в режимі передачі даних зі швидкістю 16 кбіт/с по радіолінії з ППРЧ зі швидкістю 100 стрибків за секунду) при найбільш сприятливих умовах ведення радіозв'язку ($P_{\text{зв}}$ = 0,9, m/m^* = 0,1) є низькою і становить 0,12;

оцінка ефективності функціонування СРЗ з ППРЧ за узагальненим показником ймовірності своєчасної та достовірної доставки повідомлень (надання послуг) дає можливість визначати ключові показники та критерії технічних характеристик СРЗ (за окремими методиками) та встановлювати вимоги до них, а саме:

обґрунтовувати вибір виду ППРЧ (міжбітова, побітова і внутрібітова);

визначати швидкість ППРЧ;

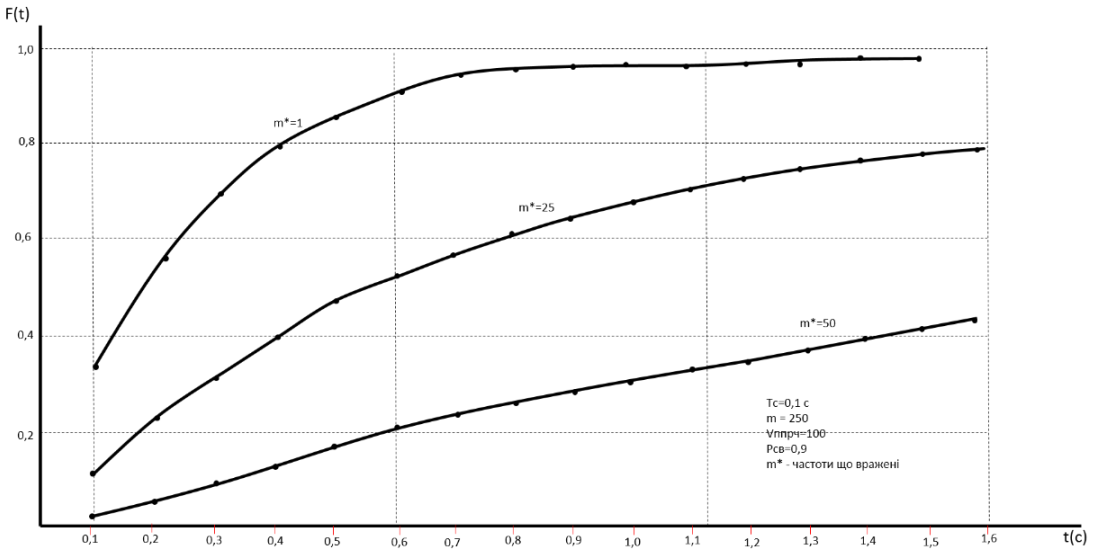

Рис.1. Оперативна ефективність радіоліній з ППРЧ без використання додаткових заходів підвищення достовірності прийому сигналів

визначати коефіцієнт розширення спектра сигналу ППРЧ, а отже обґрунтовувати вибір оптимальної адресної групи;

визначати варіанти формування адресної групи частот (в широкому діапазоні частот, у вузькому діапазоні частот, за списком);

обґрунтовувати вибір виду оптимальних сигнальних конструкцій;

визначати методи синхронізації в СРЗ з ППРЧ;

обґрунтовувати вибір виду завадостійкого кодування сигналів (наприклад, коди Ріда – Соломона, Вітербі й ін.);

визначати спосіб генерування оптимальних псевдовипадкових послідовностей частот сигналу з ППРЧ та ін.;

значне підвищення ефективності функціонування радіоліній з ППРЧ може бути досягнуто за рахунок виключення з радіообміну частот, уражених завадами (m^*).

Висновки

Запропонований метод оцінки ефективності функціонування СРЗ з ППРЧ за узагальненим показником ймовірності своєчасної та достовірної доставки повідомлень (надання послуг) дає можливість визначати ключові показники та критерії технічних характеристик СРЗ на підставі оперативно-тактичних вимог до систем управління (озброєння) та встановлювати вимоги до них.

Напрямом подальших досліджень є наукове обґрунтування вибору напрямів розвитку СРЗ спеціального призначення з урахуванням існуючих та перспективних підходів до побудови автоматизованих радіозасобів і комплексів, що реконфігуруються.

ЛІТЕРАТУРА

1. Боковик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. Санкт-Петербург: ВАС. 2006. 182 с.

2. Надежность и эффективность в технике: справочник. Н17. В 10 т. / Ред. совет: В. С. Авдуевский (пред.) и др.; Т. 3: Эффективность технических систем. Под общ. ред. В. Ф. Уткина, Ю. В. Крючкова. Москва: Машиностроение, 1988. 328 с.

3. Борисов В. И., Зинчук В. М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. Москва: Радио и связь, 1999. 252 с.

4. Torrieri DJ. Principles of secure communication systems. Dedham. MA.: Artech House Inc., 1985. 286 p.

5. Борисов В. И., Зинчук В. М., Лимарев А. Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / Под ред. В. И. Борисова. Изд. 2-е, перераб. и доп. Москва: Радио Софт, 2008. 512 с.

6. Чуднов А. М. Об адаптивных алгоритмах псевдослучайного переключения рабочих частот радиолиний в условиях случайных и преднамеренных помех. *Журнал радиоэлектроники*. 2015. № 4.

7. Беккиев А. Ю., Борисов В. И. Оценка помехозащищенности каналов радиосвязи в условиях действия помех от средств радиоэлектронной борьбы. *Радиотехника и электроника*. 2019. Том 64, № 9. С. 891–901.

8. Стогов Г. В., Елишев В. В. Помехоустойчивость систем связи с быстрой ППРЧ и кодированием в условиях шумовых помех в части полосы. *Техника средств связи.* Сер. «Техника радиосвязи». 1991. Вып. 1. С. 57–63.

9. Н.И. Козленко, А.Н. Мокроусов. Адаптивная радиолиния с псевдослучайной перестройкой рабочей частоты. Теория и техника радиосвязи. Воронеж : 2008. – 5-12 с. [Електронний ресурс]. – Режим доступу: http://www.sozvezdie.su/science/nauchnotehnicheskiy_zhurnal/. (дата звернення 17.05.2021 р.).

10. Елишев В. В, Почивалов С. Г. Метод повышения помехоустойчивости космических систем связи с быстрой псевдослучайной перестройкой рабочей частоты в условиях радиоэлектронного подавления. *Сборник трудов Военно-космической академии имени А. Ф. Можайского.* Санкт-Петербург: ВКА имени А. Ф. Можайского, 2016. С. 297−301.

11. Зинчук В. М., Щукин Н. И. Синтез подобного алгоритма многоальтернативного обнаружения при наличии мешающих параметров и неизвестных вероятностях появления обнаруживаемых сигналов. *Техника средств связи.* Серия ТРС. 1981. Вып. 7. С. 54–71.

12. Зинчук В. М., Сосулин Ю. Г., Матвеева Е. А. Синтез и анализ оптимальных алгоритмов многоальтернативного совместного обнаружения и оценивания параметров сигналов в условиях априорной неопределенности. *Техника средств связи.* Серия ТРС. 1992. Вып. 5. С. 3–30.

13. Зинчук В. М. Синтез и анализ оптимальных алгоритмов многоальтернативного совместного обнаружения и оценивания параметров сигналов при неизвестных вероятностях их появления. *Труды Международной научно-технической конференции "Авиация XXI века",* г. Воронеж, Россия, октябрь 1999 г. С. 341–361.

14. Зинчук В. М., Лимарев А. Е. Синтез и анализ инвариантных алгоритмов многоальтернативного обнаружения и различения сигналов в условиях априорной неопределенности. *Теория и техника радиосвязи*. 1996. Вып. 2. С. 32–47.

15. Гурський Т. Г. Підвищення завадозахищеності радіоліній з ППРЧ в умовах завад у відповідь. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. Вип. 3 (40). С. 58–63.

16. Чаркин Д. Ю. Сравнительный анализ помехоустойчивости и скрытности различных методов расширения спектра сигналов. Ч. 1: Помехоустойчивость / Д. Ю. Чаркин, С. Ю. Алехин, Е. В. Григорьев, А. Е. Лимарев, В. Е. Прохоров. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2017. № 4. 106 с.

17. Чаркин Д. Ю. Сравнительный анализ помехоустойчивости и скрытности различных методов расширения спектра сигналов. Ч. 2. Скрытность / Чаркин Д. Ю., Алехин С. Ю., Григорьев Е. В., Лимарев А. Е., Прохоров В. Е. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2017. № 4. 106 с.

18. Чаркин Д. Ю. Гибридные ППРЧ/ШПС системы связи. Ч. 1. Основы теории / Чаркин Д. Ю., Алехин С. Ю., Григорьев Е. В., Лимарев А. Е., Прохоров В. Е. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2017. № 3. 104 с.

19. Чаркин Д. Ю. Гибридные ППРЧ/ШПС системы связи. Ч. 2. Основы теории / Чаркин Д. Ю., Алехин С. Ю., Григорьев Е. В., Лимарев А. Е., Прохоров В. Е. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2017. № 3. 104 с.

20. Николаев В. И. Функционирование цифровых систем связи в условиях радиоэлектронного конфликта с минимаксных позиций теории игр (часть 1) / Николаев В. И., Федоров А. Е. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2010. № 2. 127 с.

21. Николаев В. И. Функционирование цифровых систем связи в условиях радиоэлектронного конфликта с минимаксных позиций теории игр (часть 2) / Николаев В. И., Федоров А. Е. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2010. № 2. 127 с.

22. Прохоров В. Е. Обоснование требований к числу частотных каналов систем радиосвязи с ППРЧ. *Теория и техника радиосвязи*. Воронеж: АО "Концерн "Созвездие", 2018. № 3. 126 с.

23. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев, Н. П. Мухин, Г. С. Нахмансон; под ред. В. И. Борисова. Москва: Радио и связь, 2003. 640 с.

24. Помехозащищенность радиосистем со сложными сигналами / Г. И. Тузов и др.; под ред. Г. И. Тузова. Москва: Радио и связь, 1985. 264 с.

25. Волков Л. Н., Немировский М. С., Шинаков Ю. С. Системы цифровой радиосвязи: базовые методы и характеристики: учеб. пособие. Москва: Эко-Трендэ. 2005. 392 с.

26. Николаев В. И., Фёдоров А. Е. Функционирование цифровых систем связи в условиях радиоэлектронного конфликта с минимаксных позиций теории игр. *Теория и техника радиосвязи.* Воронеж, 2010. С. 37–45. URL: http://www.sozvezdie.su/science/nauchnotehnicheskiy_zhurnal/ (дата звернення 17.05.2022).

27. Чуднов А. М. О минимаксных алгоритмах формирования и приема сигналов. *Проблемы передачи информации.* 1986. Т. 22. № 4. С. 49–54. URL: http://www.mathnet.ru/links/ea34d75f88c1b1281819151b04a3825e/ppi958.pdf (дата звернення 18.05.2022).

28. Гремяченский С. С., Николаев В. И. Введение в теоретико-игровой анализ радиоэлектронного конфликта систем радиосвязи со средствами радиоэлектронного подавления. *ВНИИС.* Воронеж, 1998. С. 38–49.

УДК 004.75

Драглюк О. В. ORCID: 0000-0001-8572-7257 (ВІТІ)
Радченко М. М. ORCID: 0000-0002-8272-0727 (ВІТІ)
Коротков М. М. ORCID: 0000-0002-1683-0661 (ВІТІ)
Павлюк Д. О. ORCID: 0000-0001-8461-3899 (ВІТІ)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ VIRTUAL DESKTOP INFRASTRUCTURE В ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУРАХ УЧАСНИКІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

З метою виконання завдань Стратегій національної та воєнної безпеки України щодо забезпечення упровадження сучасних інформаційних технологій, автоматизації управлінських процесів і цифровізації діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється, проводяться заходи щодо приведення існуючої інформаційної інфраструктури до сучасних вимог.

Технічна компонента інформаційної інфраструктури органів управління учасників сектору безпеки та оборони зазвичай складається з наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за практичною реалізацією в технологіях "товстого" та "тонкого" клієнтів (термінального сервера) клієнт-серверних архітектур розгортання обчислювальних мереж. В статті коротко наведені їх переваги та недоліки.

З огляду на те, що роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності цих рішень з іншого – то перебудова інформаційної інфраструктури повинна ґрунтуватися на завідомо доказаними світовою практикою у своїй ефективності технологіях.

Логічним продовженням розвитку технології термінального сервера є віртуалізація робочих столів (Virtual Desktop Infrastructure – VDI). На думку авторів статті створення віртуальних робочих станцій за робочими місцями службових осіб органів управління учасників сектору безпеки та оборони – це один ізі шляхів забезпечення якісного виконання завдань службовими особами в інфраструктурі єдиного інформаційного середовища.

В статті наданий короткий огляд продуктів вендорів, які є світовими лідерами у наданні послуг з віртуалізації, функціонально-технічних можливостей VDI, обґрунтування та шляхи упровадження наведеної технології в діючу інформаційну інфраструктуру органів управління учасників сектору безпеки та оборони.

Застосування наведеної технології дозволить існуючій архітектурі набути низки переваг за наступними напрямами: підвищення ефективності централізованого управління та надання сервісів; підвищення безпеки інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

Ключові слова: *інформаційна інфраструктура, віртуалізація робочих столів, інформаційна технологія.*

O. Draglyuk, M. Radchenko, M. Korotkov, D. Pavlyuk Application of Virtual Desktop Infrastructure technologies in special purpose information infrastructure.

In order to fulfill the tasks of the Strategies of National and Military Security of Ukraine to ensure the introduction of modern information technologies, automation of management processes and digitalization of activities in the defense forces of Ukraine with an appropriate level of information security, which is processed, measures are being taken to bring the existing information infrastructure to modern requirements.

The technical component of the information infrastructure of the security and defense sector actors usually consists of sets of information and information-analytical systems, which are different in purpose, but the same in practice in the technology of "thick" and "thin" clients (terminal server) client-server architectures deployment of computer networks. The article briefly lists their advantages and disadvantages.

Considering that the role of information technologies in management systems is to ensure the achievement of indicators of sufficient quality of management decisions by officials of management bodies, or rather: in solving the contradiction between the growing complexity, dimension, dynamism of management tasks - on the one hand, and growing requirements for efficiency, rationality, validity, effectiveness of their decisions, on the other hand, the restructuring of the information infrastructure should be based on the technology that has been obviously proven by world practice in its effectiveness.

A logical continuation of the development of terminal server technology is desktop virtualization (Virtual Desktop Infrastructure - VDI). According to the authors of the article, the creation of virtual workstations for the jobs of officials of the governing bodies of the security and defense sector is one of the ways to ensure quality performance of tasks by officials in the infrastructure of a single information environment.

The article provides a brief overview of the products of vendors who are world leaders in providing virtualization services, VDI functionality and capabilities, rationale and ways to implement this technology in the existing information infrastructure of the security and defense sector.

The application of this technology will allow the existing architecture to gain a number of advantages in the following areas: improving the efficiency of centralized management and service delivery; improving information security; flexibility in work and implementation of scaling; effective use of finances to support and develop information infrastructure; creating conditions for the transition to cloud technologies.

Keywords: *information infrastructure, desktop virtualization, information technology.*

Постановка завдання у загальному вигляді.

Реформування сфери безпеки і оборони за стандартами НАТО належить до найважливіших пріоритетів як зовнішньої, так і внутрішньої політики України. На ряду із іншими важливими заходами щодо вдосконалення систем управління, формування оборонних ресурсів та прийняття на озброєння нових зразків озброєння та військової техніки є створення сучасної інформаційної інфраструктури спеціального призначення. На законодавчому рівні підтримка цих процесів здійснюється низкою відповідних актів, в яких загострюється увага на завданнях відповідного характеру.

Для прикладу, відповідно до Указу Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України" [1] (далі – Стратегія) одним із основних напрямків зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки є здійснення цифрової трансформації, забезпечення надання адміністративних послуг через безпечне "єдине вікно" з використанням сучасних інформаційних технологій, поширення цифрової грамотності, а також визначено основним завданням системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури в умовах цифрової трансформації.

В Стратегії наведені напрями та завдання реформування й розвитку сектору безпеки і оборони. У зв'язку з цим зазначено, що зміцнення бойового потенціалу ЗС України, інших складових сил оборони можливо здійснити такими сприятливими для розвитку інформаційно-телекомунікаційних технологій (далі – ІТ-технологій) шляхами, як:

удосконалення та розвиток на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики;

посилення взаємодії органів сектору безпеки й оборони у виконанні спільних завдань;

створення системи ефективного управління та координації діяльності органів сектору безпеки і оборони, удосконалення її архітектури;

завершення створення та формування сучасних спроможностей національної системи кібербезпеки, зміцнення системи суб'єктів забезпечення кібербезпеки та координації кібероборони.

В Стратегії воєнної безпеки України [2] – наступному документі розвитку воєнної складової безпеки країни – визначена мета забезпечення реалізації державної політики у сфері оборони та пріоритетні шляхи її реалізації у сфері оборони та військового будівництва. Досягнення цілей реалізації державної політики у воєнній сфері передбачається здійснити шляхом виконання завдань за пріоритетом – запровадження об'єднаного керівництва з підготовки та ведення всеохоплюючої оборони України, зокрема:

упровадження сучасних інформаційних та космічних технологій, автоматизація управлінських процесів і цифровізація діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється.

Вирішення наведених завдань потребує здійснення цілеспрямованих, скоординованих за термінами, обсягами ресурсного забезпечення заходів щодо приведення існуючої інформаційної інфраструктури до сучасних потреб.

Аналіз останніх досліджень і публікацій.

Публікацій на тему перебудови інформаційної інфраструктури складових сил оборони з огляду на важливість питання існує достатня кількість. Нижче наведемо деякі з них.

Згідно з [3] реакція органів управління оборонного відомства України на зростаючі вимоги щодо оперативності надання інформації для прогнозування розвитку ситуацій і забезпечення оперативного управління характеризується інтенсивним впровадженням та використанням електронних систем, баз даних, реєстрів, архівів, аналітичних систем, систем моніторингу. В цьому процесі враховуються тенденції розвитку та використання інформаційних технологій в

державному секторі. Автори [3], виходячи із фінансової доцільності та технологічної можливості, зазначають необхідність створення єдиної захищеної ІТ-структури оборонного відомства, яка забезпечить централізацію всіх існуючих в МО та ЗС України інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних на базі єдиної захищеної та катастрофостійкої технологічної платформи, основним елементом (ядром) в якій пропонується використання центру обробки даних (далі – ЦОД), що забезпечуватиме роботу єдиної масштабованої, високонадійної автоматизованої відомчої системи (рис. 1).

Автори [3] відмічають, що наявність такої платформи значно полегшить створення будь-яких проєктів у сфері інформатизації та оптимізує витрати на комплексну систему захисту інформації (далі – КСЗІ).

У статті [4] на прикладі оборонного відомства показано, що протягом тривалого часу в інформаційних інфраструктурах спеціального призначення створювались та розвивались окремі автоматизовані, інформаційні, інформаційно-аналітичні та інші програмні системи, які забезпечували інформаційну підтримку лише окремих функціональних процесів управління, що сформувало такі характеристики територіально розподіленої інформаційної інфраструктури оборонного відомства країни, як відокремленість та ізольованість її складових.

Рис. 1. Компоненти єдиної захищеної відомчої ІТ-структури

Тому побудова інформаційної системи, яка функціонує у вигляді єдиної платформи та забезпечує прозоре управління функціональними процесами, гнучко адаптується під будь-які зміни, – є одним із пріоритетних завдань вдосконалення інформаційної інфраструктури не тільки ЗС України, але й складових сил оборони у цілому.

Оскільки роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності їх рішень – з іншого, то цілісна інформаційна інфраструктура має будуватися на досвіді впровадження передових інформаційних технологій, які показали свою ефективність.

Сфера застосування ІТ повинна охоплювати практично всі етапи і складові управлінської діяльності на макрорівні корпоративно-центричної моделі управління складових сил оборони та на мікрорівні – застосування зброї чи засобів ураження і є системоутворюючим фактором сучасних процесів прийняття рішення, що дозволить досягнути якісно нового етапу розвитку воєнного мистецтва – переходу від управління військами в ході конфлікту до управління конфліктом у цілому [5].

Таким чином, робота щодо пошуку ефективних шляхів впровадження нових інформаційних технологій, які практикуються світовими ІТ-спільнотами, триває, тому автори цієї статті вважають актуальним дослідження прикладних застосувань технологій Virtual Desktop Infrastructure (далі – VDI) в інформаційних інфраструктурах складових сектору безпеки та оборони.

Метою роботи є аналіз функціонально-технологічних можливостей технології VDI та обґрунтування пропозицій щодо її застосування в інформаційних інфраструктурах складових сектору безпеки та оборони.

Виклад основного матеріалу.

Виконання завдань, які забезпечуються локальними обчислювальними мережами органів управління (далі – ОУ) учасників сектору безпеки та оборони, визначаються функціональними повноваженнями службових осіб, які, як наведено в [5] на прикладі оборонного відомства, виражаються у здійсненні:

процесів оперативного планування на етапі підготовки операцій (бойових дій) щодо розподілу особового складу органу військового управління по пунктах управління та розмежування доступу службових осіб до даних, які використовуються;

формування деталізованого переліку заходів (завдань), що виконуються службовими особами структурних підрозділів штабу на етапі підготовки операцій (бойових дій);

доведення запланованих завдань до службових осіб штабу та контроль їх виконання;

формування проєктів електронних документів щодо організації роботи штабу при плануванні операцій (бойових дій);

ведення спеціалізованого військового діловодства в ОУ – автоматизована розробка, пошук і відпрацювання бойових (оперативних) документів за напрямками всебічного забезпечення і логістики;

проведення оперативно-тактичних розрахунків та інформаційно-аналітичної підтримки прийняття рішень, де передують оцінки фізико-географічних умов регіону проведення операцій (бойових дій), противника, розрахунки переміщення сил та засобів, визначення маршрутів прольоту армійської авіації тощо;

інформаційного обміну між користувачами та постачальниками інформації як в середині ОУ, так і ззовні (відповідно до категорій терміновості та прав доступу до них службових осіб, автоматизоване ведення адресних книг, журналів і формування звітної документації), реалізація вимог керівних документів щодо організації обміну інформацією;

геоінформаційного забезпечення службових осіб шляхом надійного доступу до просторових даних із поданням їх в наочній формі (електронної картографічної інформації про місцевість, автоматизація процесів створення, оновлення та підготовки до друку топографічних карт усього масштабного ряду, формування електронних карт різних масштабів, доведення до ОУ та військ (сил) електронної картографічної інформації про місцевість, об'єкти на ній, цифрових даних обстановки та ін.).

Очевидно, що робота службових осіб (далі – користувачів) в ОУ відбувається в умовах високої багатоаспектності та складності задач управління. Тому критично важливим стає забезпечення розроблення, впровадження і використання сучасних ІТ, починаючи з постановки завдань, визначення джерел отримання інформації, застосування математичних засобів інформаційно-аналітичної підтримки до створення цілісної інформаційної інфраструктури складових сектору безпеки та оборони.

Відповідно, під кожен напрямок діяльності створювались свої підсистеми автоматизованого управління, основою яких є клієнт-серверна архітектура розгортання. Як наведено в [3; 5], технічна компонента інформаційної інфраструктури ОУ може складатися із

таких наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за принципами побудови технологічних платформ, як: підсистема організації роботи штабу, підсистема електронного документообігу, інформаційно-довідкова підсистема, інформаційно-розрахункова підсистема, підсистема інформаційного обміну, геоінформаційні системи, інформаційно-аналітична система автоматизованого обліку особового складу, інформаційно-аналітична система обліку майна (житла) та ін.

Коротко кажучи, традиційні клієнт-серверні архітектури розгортання обчислювальних мереж, в яких є сервери – вузли-постачальники деяких специфічних функцій (сервісів) і клієнти – споживачі цих функцій, в практичній реалізації набуті технологіями “товстого” та “тонкого” клієнтів.

Кожна з них визначає власні або використовує наявні правила взаємодії між клієнтом і сервером (протоколами взаємодії). Переваги і недоліки наведених технологій розглянемо нижче.

1. Архітектура розгортання “товстий клієнт” (рис. 2).

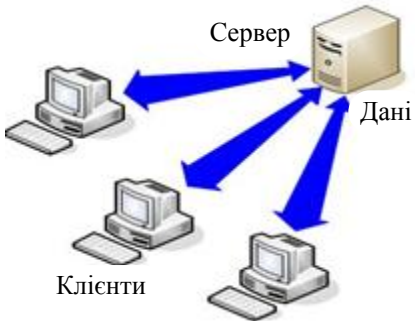

Рис. 2. “Товстий клієнт” – робоча станція або ПК, що працює під управлінням власної дискової ОС і має необхідний набір ПЗ

“Товстий клієнт” в архітектурі “клієнт-сервер” являє собою клієнтський мережевий додаток, запущений під керуванням локальної (дискової) операційної системи (далі – ОС), що забезпечує (на противагу тонкому клієнтові) повну функціональність і незалежність від центрального сервера. При цьому можливе забезпечення роботи багатьом користувачам навіть при обривах зв’язку із сервером. Такий додаток поєднує компонент подання даних (графічний користувальницький інтерфейс ОС) і прикладний компонент (обчислювальні потужності комп’ютера клієнта). Часто сервер у цьому випадку є лише сховищем даних, а вся робота по обробці та поданню даних переноситься на персональний комп’ютер (далі – ПК) користувача. До мережевих серверів “товсті клієнти” звертаються в основному за додатковими послугами (наприклад, доступ до web-серверу чи до відомчої бази даних).

Переваги:

наділений широкою функціональністю на відміну від тонкого клієнта;

можливість автономної роботи навіть при обривах зв’язку із сервером;

висока швидкодія (залежить від технічних характеристик робочої станції користувача).

Недоліки:

ускладнене адміністрування прикладних функцій через відсутність централізації;

великий розмір дистрибутива;

проблеми з віддаленим доступом до даних, що виражаються у складності відновлення даних, узгодження їх з іншими клієнтами і пов'язаної з цим не актуальністю даних;

ресурсозатратне обслуговування робочих місць (установка, налаштування і супроводження життєвого циклу, необхідність оновлення ліцензійного програмного забезпечення (далі – ПЗ) та відповідного апаратного забезпечення, кібернетичного захисту на кожному робочому місці);

ускладнений і ресурсозатратний контроль виконання політики безпеки або збільшення її вартості при територіальному розосередженні підрозділів;

висока вартість виконання вимог КСЗІ при мобільному виконанні робочого місця чи здійсненні масштабування.

2. Архітектура термінальний сервер (“тонкий клієнт”) (рис. 3).

Суть полягає в розміщенні додатків на одному сервері відразу для двох і більшої кількості користувачів. Користувачі отримують “хмарний” доступ до певних додатків і спеціалізованих програм. Клієнт лише виводить віддалений користувацький інтерфейс, що фізично розміщений на сервері.

В термінальному доступі всі співробітники отримують доступ до однієї ОС і одному набору додатків на всіх через відомчу мережу або Інтернет. (Наприклад, так працюють з програмою
1С-Підприємство).

Серверні обчислення із тонким клієнтом (SBC) або служба віддаленого робочого столу (RDS) дозволяють користувачу віддалено підключатися до програми, яка працює на серверній інфраструктурі, яка розміщена у ЦОД. Далі доставка додатків здійснюється шляхом їх встановлення та запуску на самому сервері. У цьому випадку використовують багатокористувацьку версію програми, яка затребувана для створення окремих сеансів роботи користувачів. Кожен користувач підключається до власного окремого, та захищеного сеансу цієї програми через свій термінал.

При термінальному доступі створюються окремі облікові записи всіх користувачів, які надають доступ до одночасної роботи в єдиній ОС таким чином, щоб користувачі не створювали завад один одному. На клієнтські комп’ютери встановлюються спеціальні додатки, які дають користувачам можливість працювати з окремими сесіями на термінальному сервері. При цьому слід пам’ятати, що у зв’язку з тим, що не всі виробники випускають програмні продукти, які здатні працювати в термінальному режимі, то в такому випадку, нема можливості запускати будь-який додаток.

Основна функціональна можливість, яку надає термінальний сервер – це віддалений доступ до додатків ОС, які встановлені на сервері. У користувача на пристрої повинна бути встановлена програма-клієнт, яка здійснює підключення терміналу до термінального сервера. Найпростіший приклад – програма “Підключення до віддаленого робочого столу”, яка вбудована в будь-яку ОС Windows. Доступ може бути надано або до всього робочого столу, або до певного додатку, який відкривається у так званому безшовному вікні. У першому випадку на екрані користувача запуститься термінальна сесія, яка і “закриє” собою поточний робочий стіл. У другому випадку для користувача не буде навіть помітно, що програма, яка запущена в окремому вікні, не з його ПК, а на сервері.

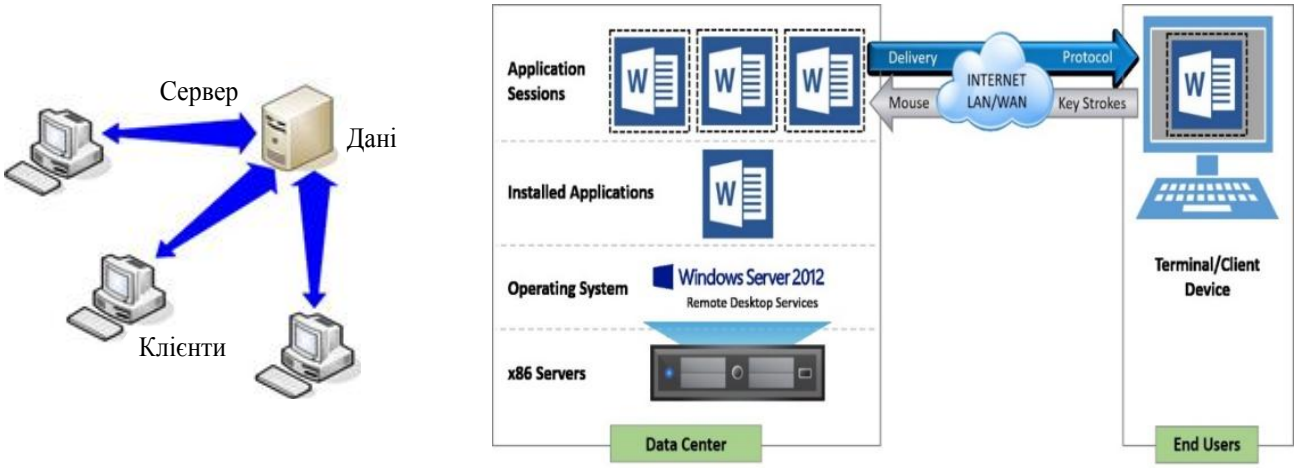

Рис. 3. Робота “тонкого клієнту” в сесії застосунку Word ОС Windows

Переваги:

централізоване управління;

просте адміністрування, дешевше розгортання;

масштабованість;

безпека, захищеність файлів (дані зберігаються на сервері);

зменшення витрат на модернізацію обладнання (клієнтські термінали потребують менших витрат на утримання за рахунок збільшеного терміну роботи);

економія трафіку у WAN-мережах, і як наслідок, зменшення затребуваної пропускної спроможності і вартості трафіку, що орендується. У випадку з термінальним доступом трафік,

який раніше проходив між клієнтськими станціями і серверами, замінюється на трафік передачі зображення на віддалений екран користувача.

Недоліки:

непрацездатність сервера може зробити непрацездатною всю обчислювальну мережу;

не можна створити повністю ізольоване середовище з окремим набором прав і програм.

Ізоляція відбувається на рівні сесії, і якщо додаток одного з користувачів викликає збій на рівні ОС, то разом із винуватцем, який викликав збій, будуть змушені перезавантажувати свої додатки й інші користувачі, які працюють на цьому ж сервері.

Деякі виробники не підтримують програмні продукти в термінальному середовищі, наприклад, Autodesk AutoCAD, а для деякого ПЗ необхідні права адміністратора.

Разом із тим загально-світові тенденції розвитку ІТ-технологій [6] дають змогу констатувати факт еволюції статичних комп'ютерних систем до віртуальних за рівнями, які наведені на рис. 4.

Рис. 4. Еволюція системного підходу побудови ІТ-інфраструктури

Говорячи про технології віртуалізації, які стали невід'ємною частиною сучасних ІТ-інфраструктур державних секторів, необхідно зазначити, що на перше місце виходять питання побудови високопродуктивної, масштабованої, ефективно керованої та безпечної інфраструктури.

У різних країнах із різною швидкістю відбувалося впровадження нових систем, а також оптимізація витрат на підтримку існуючих. Україна не є виключенням і фактично на теперішній час триває перший етап практичного застосування засобів віртуалізації, який можна охарактеризувати як "застосування віртуалізації в умовах існуючої ІТ-інфраструктури". Наступним етапом буде зміна компонентів самої інфраструктури з урахуванням можливостей віртуалізації, як нинішніх, так і перспективних.

Логічним продовженням розвитку технології термінального сервера стала віртуалізація робочих столів (VDI) – створення віртуальних робочих станцій за робочими місцями користувачів, що і пропонується авторами дійсної статті як один із шляхів забезпечення якісного виконання завдань службовими особами ОУ.

Розглянемо детальніше особливості VDI.

3. "Тонкий клієнт" в технології VDI.

VDI – це концепція, в якій дані з ПК користувача зберігаються централізовано на сервері в ЦОД, а у кожного користувача ПК – віртуальний. Розгортається особлива інфраструктура для віддаленої роботи, при якій на основі одного фізичного сервера створюється кілька віртуальних, що дозволяє запускати дві і більше ОС у віддаленому режимі. З архітектурної точки зору, адміністратор сервера для паралельної роботи кожного користувача створює віртуальний повноцінний робочий стіл з окремим набором додатків, програм, документів і доступів. Операційна система, профіль користувача, політики настільних ПК та програми обробляються як окремі компоненти, які абстрагуються від базової машини, а потім передаються разом з метою створення робочих столів користувачам. Підключення і вся робота користувачів йде через “прошарок” – “тонкий клієнт” (рис. 5).

Замість того, щоб підключатися до відокремленого, захищеного індивідуального сеансу програми, користувач тепер підключається до відокремленого, захищеного, індивідуального примірника ОС сервера, в якому містяться затребувані застосунки.

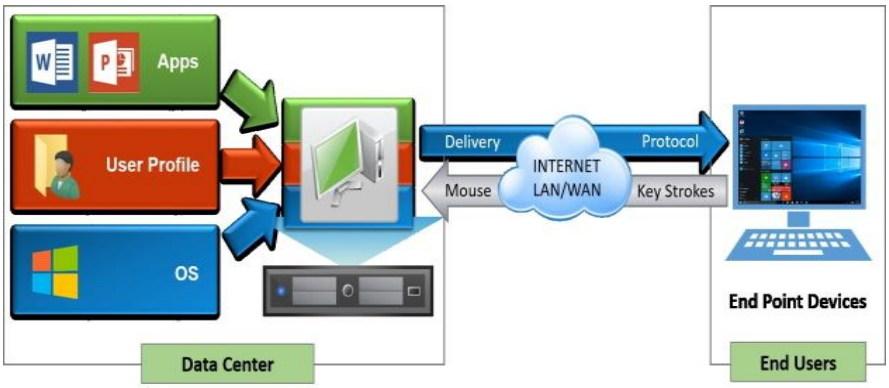

Рис. 5. Набір компонентів віртуального робочого столу для “тонкого клієнта”

Існує два типи інфраструктури VDI: зі збереженням стану і без збереження стану. У випадку зі збереженням стану користувачеві надається певний віртуальний робочий стіл, до якого він може постійно підключатися і котрий він може налаштувати відповідно до своїх потреб, оскільки зміни зберігаються після скидання підключення. Іншими словами, віртуальний робочий стіл у VDI зі збереженням стану працює аналогічно фізичному комп’ютеру. Інфраструктура VDI без збереження стану, в якій користувачам надаються стандартні віртуальні робочі столи і зміни не зберігаються, є більш простим і дешевшим варіантом, оскільки немає необхідності зберігати налаштування віртуальних робочих столів після завершення сеансу. Цей спосіб VDI часто використовується в організаціях із великою кількістю співробітників, що виконують стандартні завдання або при вирішенні обмеженої кількості завдань, що повторюються, для яких не потрібно налаштовувати віртуальні робочі місця.

Відповідно до [7], 80 % світових організацій вже включили технологію VDI у стратегії розвитку інформаційно-телекомунікаційних інфраструктур і які очікують прогнозоване зменшення адміністративних витрат на 70 %, на електроенергію – 97 %, а дозвіл працювати своїм 70 % співробітникам з мобільних пристроїв з будь-якого місця і в будь-який час – дасть на 98 % збільшення продуктивності їх роботи.

Впровадження VDI в роботу службових осіб в ОУ учасників сектору безпеки та оборони із врахуванням обмежень державного регулятора із захисту інформації теж може бути доцільним і обґрунтованим за нижче наведеними напрямками.

Централізація ІТ-сервісів. Перехід до “хмарної” моделі обслуговування. Оскільки зростання пропускної здатності каналів передачі даних і якості сервісів дозволяє уникнути необхідності їх розміщення в безпосередній близькості від користувачів, створюється можливість здійснення централізації ІТ-сервісів в одному чи декількох ЦОД або створення умов переходу до “хмарної” моделі обслуговування. Перехід до такої моделі можливий, оскільки обмін великого об’єму частини трафіку між користувацькими додатками здійснюється в середині серверів ЦОД, а на робоче місце користувача передаються лише дані, що змінилися.

Централізоване управління. Спрощення підтримки та оновлення робочих місць. Централізовані робочі столи на рівні із централізованим управлінням для 1-2 адміністраторів (незалежно від їх територіального розміщення у мережі) дають можливість для кожного робочого столу виконувати набагато простіше такі завдання, як: резервне копіювання, оновлення ПЗ, налаштування ОС чи встановлення нових програм. Контроль за діями користувачів, керування різнорідним парком апаратного забезпечення відбувається з однієї точки мережі. Технологія VDI дозволяє створювати віртуальні робочі столи з єдиного образу, що підтримується та оновлюється централізовано, а також надає гнучкості при переході на нові версії ОС, оскільки не вимагає негайної відмови від існуючої ОС або заміни клієнтського пристрою.

Організація віддаленої роботи. Гнучкість в роботі та масштабованість. За допомогою VDI можливе забезпечення доступу до будь-якої програми, навіть якщо користувачі знаходяться за межами контрольованої зони відомчої мережі та не мають доступу до своїх робочих місць. На відміну від термінального доступу, VDI дозволяє запустити більш широкий спектр додатків завдяки використанню клієнтських версій ОС. За рахунок ізоляції робочих середовищ користувачів на рівні віртуальних машин (далі – ВМ), для кожної ОС і користувача можуть бути виконані індивідуальні налаштування, що не перемежовуються з іншими користувачами, наприклад, деяким з них можуть надаватися права локальних адміністраторів. Технологія VDI дозволяє гнучко змінювати апаратну конфігурацію ВМ, швидко створювати або повторно розгортати віртуальні робочі столи, що доречно у разі територіально-розподіленої роботи окремих підрозділів, наприклад, у випадку коли немає можливості оперативно доставити користувачу нову робочу станцію або за відсутності у філіальному підрозділі підмінного фонду комп'ютерів і комплектуючих.

Заощадження операційних витрат. Впровадження середовища віртуального робочого столу разом із найкращими практиками щодо управління зображеннями, виправленнями та профілями за допомогою централізованого розгортання додатків призведе до економії операційних витрат порівняно з традиційним управлінням робочих столів. Капітальні витрати на початку проєкту VDI будуть вищими у міру розгортання інфраструктури, проте зниження операційних витрат будуть пов'язані із: закупівлею ліцензій на ПЗ (завдяки встановленню набору користувацьких додатків не на кожен ПК, а на один сервер); зменшеними затратами на електроенергію (завдяки зниженню електроспоживання клієнтських пристроїв до рівня 7–15 Вт); модернізацією парку обчислювальної техніки (завдяки витратам тільки на серверну частину, більш тривалого терміну експлуатації тонких або нульових клієнтів); зменшенням штату технічної підтримки; обслуговуванням і ремонтом системи у цілому.

Підвищення безпеки інформації. Технологія VDI задовольняє потреби, які висуває діяльність користувачів без компрометації безпеки, контролю, керованості та здійснює відповідність вимогам щодо нормативних обмежень державного регулятора із захисту інформації. При кожному підключенні користувача до свого віртуального робочого столу завжди створюється нова ВМ з налаштуваннями особистого оточення. У разі зараження шкідливим ПЗ досить просто перепідключитися до свого віртуального робочого столу, в результаті чого під користувача буде автоматично створена нова ВМ з особистими налаштуваннями оточення, груповими політиками й особистими файлами.

Завдяки централізованому зберіганню призначених для користувачів даних VDI дозволяє спростити механізми резервування й аварійного відновлення робочих столів. Технологія дозволяє реалізувати різні сценарії катастрофостійкості, наприклад, із використанням територіально-розподілених кластерів, автоматичного перемикання на резервний ЦОД або виділення користувачам двох віртуальних робочих столів у різних ЦОД.

Очевидно, що виконання вимог щодо захисту інформації повинно здійснюватися в рамках впровадження хмарних обчислень в державні інформаційні інфраструктури учасників сектору безпеки та оборони, як наведено в [8; 9].

Недоліки VDI. Основним недоліком, що перешкоджає широкому поширенню VDI, залишається висока вартість впровадження порівняно з фізичними робочими станціями або термінальним доступом [10]. Чималу частку у вартості відіграють ліцензії на ПЗ віртуалізації,

ОС Windows і брокери VDI. Наприклад, на теперішній час для легального використання клієнтських ОС Windows потрібно або мати ліцензію Windows з чинним Software Assurance на кожен пристрій, з якого здійснюється підключення до віртуальних робочих столів, або щорічну передплатну підписку Windows VDA. До цього додаються витрати на серверні ОС Microsoft Windows і в ряді випадків Microsoft SQL Server, що потрібно для функціонування більшості VDI рішень, а також вимоги щодо ліцензування брокерів VDI (як правило, за кількістю користувачів або активних підключень).

Витрати на апаратне забезпечення. При реалізації у відомстві сценарію інсталяції наведеної технології не з нуля (при збільшені кількості робочих місць, при масовій модернізації) у випадку, коли вже є в наявності достатня кількість функціонуючих ПК, їх можна використати як «тонкі клієнти» після здійснення відповідних доналаштувань. Водночас, для запуску великої кількості віртуальних робочих столів (їх зберігання) потрібне здійснення достатньо затратного апаратного забезпечення, такого як: високопродуктивних серверів із багатоядерними процесорами та великим об'ємом оперативної пам'яті; виділені системи зберігання даних, які здатні надавати необхідні обсяги дискового простору і з високими характеристиками IOPS (кількість операцій введення/виводу в секунду), щоб забезпечити як типові навантаження, так і періодичні пікові; клієнтських терміналів, які необхідні для розгортання VDI.

Клієнтські пристрої («тонкі» клієнти) залишаються вельми недешевим задоволенням. За ціну брендового «тонкого» клієнта (далі – ТК) можна придбати ПК початкового рівня, достатнього для вирішення типових офісних завдань. Крім того, для роботи деяких функцій VDI (підключення сканерів, інтеграція з VOIP-клієнтами та ін.) може знадобитися придбання ТК з ОС Windows Embedded/IOT, що відрізняється більш високою вартістю.

Вимога доступу до мережі. VDI, як і переважна більшість сучасних IT-сервісів, вимагає наявності надійного високошвидкісного мережевого доступу до ЦОД. Незважаючи на розвиток бездротового та мобільного Інтернету, далеко не завжди швидкість і стабільність підключення задовільняють комфортну роботу.

Рівень підготовки кваліфікованих спеціалістів ІТ. Якщо для управління фізичними робочими станціями досить фахівця початкового рівня, то для організації VDI потрібно спеціально підготовлений співробітник або група, які б розбиралися у платформах віртуалізації. Огляд компаній-вендорів, які надають послуги VDI, що наведений у звіті компанії IDC Market Scape щодо проведених досліджень ринку надання послуг VDI за 2019–2020 роки [11] свідчить, що лідерами ринку є: Citrix і VMware. Решта – це учасники другого ешелону: Microsoft, Amazon, Parallels, CloudJumper, Huawei та ін.

Доцільно коротко зупинитись на продуктах Citrix і VMware. В мережі Інтернет достатньо порівнянь як відносно незалежних, так і ангажованих за одну чи іншу сторону [12–14]. Якщо говорити про кожного лідера окремо, то VMware може бути цікавим завдяки широкому набору власних продуктів і рішень, які є у складі бандла Horizon або інтегруються з ним. VMware надає найбільш повний і функціональний набір продуктів, на якому можливо побудувати закінчену VDI інфраструктуру з нуля. VMware виходить вперед завдяки реалізації в Horizon таких можливостей, які раніше були сильними сторонами Citrix – доставці додатків з термінальних серверів, а також протоколу Blast, який оптимізований для роботи через повільні, ненадійні канали.

З іншого боку, компанія Citrix зайняла частину ринку завдяки поширеності рішень з організації термінального доступу XenApp, а також пропозицій широких можливостей щодо інтеграції з різними платформами віртуалізації (власний гіпервізор Citrix XenServer, Microsoft Hyper-V, Nutanix AHV і VMware vSphere) чи із хмарними сервісами інших вендорів – Microsoft Azure і Amazon AWS. Забезпечення крос-платформеності і партнерство з іншими виробниками систем віртуалізації є сильними сторонами Citrix.

Висновки. Таким чином, наведені функціонально-технологічні можливості VDI – створення віртуальних робочих столів за робочими місцями службових осіб органів управління – учасників сектору безпеки та оборони, дозволять набути переваг існуючим інформаційним інфраструктурам за наступними напрямками: централізоване управління та надання сервісів;

безпека інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

В реаліях сьогодення впровадження засобів віртуалізації проводитиметься в умовах діючої ІТ-інфраструктури. Найдоцільнішим варіантом забезпечення міграції буде здійснення переналаштування визначеного парку ПК в тонкі клієнти, резервування серверів в ЦОД, оплати ліцензій ПЗ обраного вендора, налаштування високошвидкісних каналів передачі даних, задання відповідного алгоритму переходу на VDI водночас із паралельним процесом закінчення життєвих циклів існуючих ІТС. Переваги технології VDI, які наведені в статті, – очевидні, проте постає питання правильної оптимальної конфігурації для різних пунктів управління, переліку функціональних сервісів, які надаватимуться відповідним службовим особам, що і буде напрямком подальших досліджень.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України": Указ Президента України від 14.09.2020 № 392/2020 // Офіс Президента України: офіційний портал. URL: https://www.president.gov.ua/news/volodimir-zelenskij-zatverdiv-strategiyu-nacionalnoyi-bezpek-63577 (дата звернення: 02.04.2022).

2. Про рішення Ради національної безпеки і оборони України "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.2022 № 121/2022. // Офіс Президента України: офіційний портал. URL: https://www.president.gov.ua/documents/1212022-37661 (дата звернення: 02.04.2022).

3. Гудима О. П. ІТ-структура армії / О. П. Гудима, О. Б. Шиятий. *Оборонний вісник.* Київ, 2016. № 8. С. 4–7. URL: https://issuu.com/defensebulletin/docs/ov_08_2016_ukr (дата звернення: 02.04.2022).

4. Кірпічніков Ю. А. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами / Ю. А. Кірпічніков, О. В. Андрощук, О. В. Головченко, М. В. Петрушен. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* Київ, 2019. № 1 (65). С. 86–91.

5. Пермяков О. Ю. Організація інформаційних систем Збройних Сил України: навч. посіб. / О. Ю. Пермяков, Н. О. Королюк, С. І. Фараон. Київ: Національний університет оборони України імені Івана Черняховського, 2019. 134 с.

6. Колесов А. Виртуализация инфраструктуры – ключевое направление в ИТ // Портал "itWeek". 31.05.2011. URL:. https://www.itweek.ru/infrastructure/article/detail.php?ID=131652 (дата звернення: 02.04.2022).

7. Бараш Л. Инфраструктура виртуального десктопа. Почему технология VDI становится популярнее в отечественном корпсекторе? // Компьютерное Обозрение. 25 червня 2019 р. URL: https://ko.com.ua/infrastruktura_virtualnogo_desktopa_pochemu_tehnologiya_vdi_stanovitsya_populyarnee_v_otechestvennom_korpsektore (дата звернення: 02.04.2022).

8. Драглюк О. В. Аналіз можливостей хмарних технологій при застосуванні в інформаційній інфраструктурі складових сил оборони / О. В. Драглюк, Є. І. Нерознак, М. М. Радченко, М. М. Коротков. *Збірник наукових праць ВІТІ.* Київ, 2022. № 1.

9. Аксенов В. Архитектура G-Cloud в облаках // Ассоциация "BISA". 21 октября 2016 р. URL: https://bis-expert.ru/articles/54528 (дата звернення: 02.04.2022).

10. Коновалов А. Немного о дизайне VDI // Blogger: блог, посвященный технологиям виртуализации и смежным с ними областям. 04.09.2017. URL: http://blog.vmpress.org/2017/09/vdi-1.html (дата звернення: 02.04.2022).

11. Звіт IDC MarketScape: Worldwide Virtual Client Computing 2019–2020 Prondor Assessment" (Doc # US45752419, січень 2020). URL: https://www.idc.com/getdoc.jsp?containerId=US45752419 (дата звернення: 02.04.2022).

12. Порівняйте віртуальні програми та настільні комп'ютери Citrix та VMware Horizon View // Портал інтернет-видання IT-Central Station Unbiazed reviews from the tech community. URL: https://www.itcentralstation.com/products/comparisons/vmware-horizon-view_vs_xendesktop (дата звернення: 02.04.2022).

13. Компанія Citrix: вебсайт. URL: https://www.citrix.ru/products/xenapp-xendesktop/ compare.html (дата звернення: 02.04.2022).

14. Компанія VMware: вебсайт. URL: https://www.vmware.com/company/why-choose-vmware/workspace-transformation.html (дата звернення: 02.04.2022).

УДК 621.391

канд. техн. наук Залужний О. В. (ВІТІ)
д-р техн. наук, ст. наук. співр. Чевардін В. Є. (ВІТІ)
Артемчук М. В. (ВІТІ)
Андрєєв А. О. (ВІТІ)

ШЛЯХИ ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ОДНОСТОРОННІХ РАДІОКАНАЛІВ

При функціонуванні сучасних інформаційно-комунікаційних систем з використанням односторонніх радіоканалів основним завданням є максимізація достовірності та інформаційної скритності передачі повідомлень. Більшої актуальності це завдання набуває в умовах впливу засобів радіоелектронної боротьби та зростання числа інцидентів, пов'язаних з експлуатацією вразливостей бездротових технологій. Його розв'язання є корисним при використанні технологій інтернету речей з односторонніми протоколами взаємодії, розгортанні систем управління безпілотними літальними апаратами в рамках організації та забезпечення кіберзахисту об'єктів критичної інфраструктури держави.

Метою роботи є визначення шляхів підвищення достовірності передачі повідомлень в інформаційно-комунікаційних системах з використанням односторонніх радіоканалів.

У статті наведено приклади застосування цифрових методів модуляції та завадостійкого кодування в сучасних інформаційно-комунікаційних технологіях з односторонньою радіопередачею. Отримано результати аналізу ефективності використання цифрових методів модуляції та завадостійкого кодування за критерієм мінімуму значення ймовірності помилки на біт. Розглянуто особливості застосування комбінованого випадкового кодування, яке передбачає використання поєднання завадостійкого і стохастичного кодування.

З використанням програми NIST Statistical Test Suite 2.1.2 здійснено тестування стандартизованих генераторів псевдовипадкових послідовностей.

Результати досліджень обґрунтовують доцільність використання сигналів з бінарною відноснофазовою маніпуляцією в поєднанні з мажоритарним кодуванням для підвищення достовірності прийому повідомлень при односторонній радіопередачі. В цьому випадку ми повинні розв'язати завдання щодо вдосконалення існуючих схем оцінки фази прийнятого сигналу та оптимального вибору надлишковості мажоритарного кодування.

Для одночасного підвищення достовірності прийому повідомлень та забезпечення скритності передачі інформації запропоновано застосування принципу комбінованого випадкового кодування. При цьому для формування кодової книги доцільно використовувати Blum-Blum-Shub генератори псевдовипадкових послідовностей. За результатами тестування пакетом NIST Statistical Test Suite був обраний Blum-Blum-Shub генератор.

Ключові слова: *одностороння радіопередача, достовірність передачі повідомлень, цифрові методи модуляції, комбіноване випадкове кодування.*

Zaluzhnyi O., Chevardin V., Artemchuk M., Andreiev A. Ways to improve the reliability of message transmission in information and communication systems that use one-way radio channels.

Modern information and communication systems which use one-way radio channels have the main task to maximize the reliability and information transmission stealth. This task becomes more relevant in conditions of the radio-electronic warfare and growing of the cyber incidents with wireless vulnerabilities exploitation. This solution is useful for Internet of Things technologies with one-way interaction protocols and unmanned aerial vehicle control systems for organization and critical infrastructure cyber security support.

The purpose of this work is the fading of possible ways for increasing of the message transmission reliability in the information and communication systems with one-way radio channels.

The examples of digital modulation methods applications, interference-resistant coding which are used in modern information and communication technologies with one-way radio transmission are considered in the article. In the work were received results of digital modulation methods and interference-resistant coding analysis with minimum bit error rate criterion. The usage futures of combined random coding which is based on interference-resistant and stochastic coding combination were researched.

Standard random bit generators were tested by the NIST Statistical Test Suite 2.1.2 application.

This research results give us the possibility to increase the reliability of message transmission by way using binary phase-shift keying in combination with majority coding. In this case we should solve tasks to improve the phase estimation schemes of received signal and optimal choice of majority coding redundancy.

In order to increase the reliability and information stealth of message transmission the using of combined random coding was proposed. At the same time, we recommend to use Blum-Blum-Shub random bit generator for the codebook creating. Blum-Blum-Shub random bit generator was chosen according to estimation results, obtained with the help of NIST Statistical Test Suite.

Keywords: *one-way radio transmission, reliability of message transmission, digital modulation methods, combined random coding, information transmission stealth.*

Постановка завдання в загальному вигляді. В наш час активно розвиваються системи телеметрії, моніторингу віддалених об'єктів та оповіщення, засоби дистанційного управління безпілотними літальними апаратами (БпЛА), системи збору інформації з індикаторів кіберінцидентів, в яких окреме місце знаходить одностороння радіопередача. При функціонуванні таких систем основним завданням є підвищення достовірності та інформаційної скритності передачі повідомлень. Більшої актуальності ця задача набуває в умовах впливу засобів радіоелектронної боротьби (РЕБ) та зростання числа інцидентів, пов'язаних з уразливістю криптографічних додатків і програмних засобів, таких як CVE-2022-21449, CVE-2022-23806, CVE-2020-9283, CVE-2016-6303, CVE-2018-6594. Останнє є особливо важливим при проведенні спеціальних операцій, організації кіберзахисту об'єктів критичної інфраструктури держави, коли здійснюється передача інформації, зокрема і радіоканалами. Тому актуальним завданням є визначення можливих шляхів підвищення достовірності передачі повідомлень односторонніми радіоканалами.

Аналіз останніх публікацій.

Результати проведеного аналізу наукових досліджень у даній предметній області свідчать про те, що для підвищення достовірності прийому повідомлень при односторонній радіопередачі застосовується повторна передача повідомлень як на одній частоті, так і на наборові частот, використовуються коригуючі коди з виправленням помилок [1–5]. Такі способи є ефективними в умовах відсутності зворотного каналу зв'язку, проте мають достатньо високу та фіксовану надлишковість. Недостатньо дослідженим залишається напрямок, що пов'язаний з оцінкою особливостей застосування цифрових методів модуляції та завадостійкого кодування з метою визначенням можливих шляхів підвищення достовірності прийому повідомлень в системах з односторонньою радіопередачею. Останнє є особливо важливим для LPWAN (Low Power Wide Area Networks) систем з односторонніми протоколами взаємодії, в яких використовується ультравузькосмуговий діапазон частот, а швидкість передачі інформації не перевищує 100 біт/с [1; 2].

Мета статті: визначення шляхів підвищення достовірності передачі повідомлень в інформаційно-комунікаційних системах (ІКС) з використанням односторонніх радіоканалів.

Виклад основного матеріалу.

В якості прикладів систем з односторонньою радіопередачею розглянуто технології Internet of Things (IoT) з односторонніми протоколами взаємодії (технологія Sigfox та Weightless-N).

Технологія Sigfox [1] підтримує як односторонній, так і двосторонній режими роботи. В односторонньому режимі передача інформації здійснюється тільки висхідною лінією. Для досягнення великої дальності зв'язку при обмеженій потужності передавача (максимальна потужність передавача становить 25 мВт) система функціонує в ультравузькосмуговому діапазоні частот. Ширина смуги частот каналу висхідної лінії зв'язку становить 100 Гц (в Європі). Бітова швидкість на фізичному рівні – 100 біт/с (в Європі). Використовується differential binary phase-shift keying (DBPSK) маніпуляція. Завадостійкі коди з виправленням помилок не застосовуються [6].

Технологія Weightless-N [2] повністю базується на односторонній радіопередачі висхідною лінією. Всі пристрої відправляють повідомлення на центральну базову станцію без синхронізації та підтвердження. В системі використовується DBPSK маніпуляція в поєднанні зі згортковим кодом, що дозволяє виправляти помилки [7]. Виділений діапазон частот розподілений на шість широких смуг (табл. 1).

Таблиця 1

Смуги частот технології Weightless-N

Група №	Нижня смуга, МГц	Верхня смуга, МГц	Смуга частот, МГц	Кількість каналів
1	863	864,998	1,998	9990
2	865	868	3	15000
3	868	868,6	0,6	3000
4	868,7	869,2	0,5	2499
5	869,4	869,64	0,24	1200
6	869,7	870	0,3	1500

Кожна смуга призначена для окремої базової станції. Кінцеві пристрої працюють в вузькій смузі частот 200 Гц (мікроканал). Окрім того, кожна широкосмугова мережа ділиться на три підсмуги (макроканали), кожен з яких містить декілька мікроканалів. Наприклад, кожен макроканал в діапазоні 0,6 МГц містить 1000 каналів. Максимальна швидкість передачі даних – 100 біт/с. Таким чином, вказані системи функціонують в умовах обмеженого часового, частотного та енергетичного ресурсу. В них використовується бінарна відноснофазова маніпуляція. Підвищення достовірності прийому повідомлень шляхом застосування завадостійких кодів можливе тільки за рахунок зменшення швидкості передачі інформації (інформаційної швидкості).

Для визначення шляхів підвищення достовірності передачі повідомлень необхідно проаналізувати можливість використання різних методів маніпуляції в розглянутих системах. З цією метою було здійснено розрахунки середнього значення ймовірності помилки на біт в каналі з білим гаусовим шумом та в релеєвському каналі.

При когерентній (КГ) обробці сигналів з binary phase-shift keying (BPSK), binary frequency shift keying (BFSK) та binary amplitude shift keying (BASK) маніпуляцією ймовірність помилки на біт ($p_{\text{біт}}$) визначається за узагальненою формулою [8]:

$$p_{\text{біт}} = \text{Q}(\sqrt{\alpha\gamma_{\text{біт}}}), \tag{1}$$

де коефіцієнт α = 2 (сигнали з BPSK), α = 1 (сигнали з BFSK), α = 0,5 (сигнали з BASK);

$\gamma_{\text{біт}} = E_{\text{біт}}/N_0$ – відношення енергії біта $E_{\text{біт}}$ до спектральної щільності потужності шуму N_0;

$Q(x)$ – функція, яка використовується для визначення площі під частиною гаусівської функції щільності розподілу ймовірностей.

Ймовірність помилки на біт для КГ приймання сигналів з DBPSK розраховується за наступним аналітичним виразом [9]:

$$p_{\text{біт}} = 2\text{Q}\left(\sqrt{2\gamma_{\text{біт}}}\right)\cdot\left(1-\text{Q}\left(\sqrt{2\gamma_{\text{біт}}}\right)\right). \tag{2}$$

Ймовірність помилки на біт при некогерентній (НКГ) DBPSK визначається за формулою [9]:

$$p_{\text{біт}} = 0{,}5\cdot\text{e}^{-\gamma_{\text{біт}}}. \tag{3}$$

Результати розрахунків за формулами (1)–(3) наведено на рис. 1, з яких видно, що найменша ймовірність помилки забезпечується при використанні сигналів з фазовою або відноснофазовою (при КГ чи НКГ прийомі) маніпуляцією. Перехід від BPSK до DBPSK призводить до погіршення достовірності, яке стає все суттєвішим зі зменшенням відношення сигнал-шум (ВСШ) (при $p_{\text{біт}} = 10^{-1}$ енергетичний програш становить 2 дБ (рис. 1)). Використання когерентної DBPSK порівняно з некогерентною дає незначний виграш.

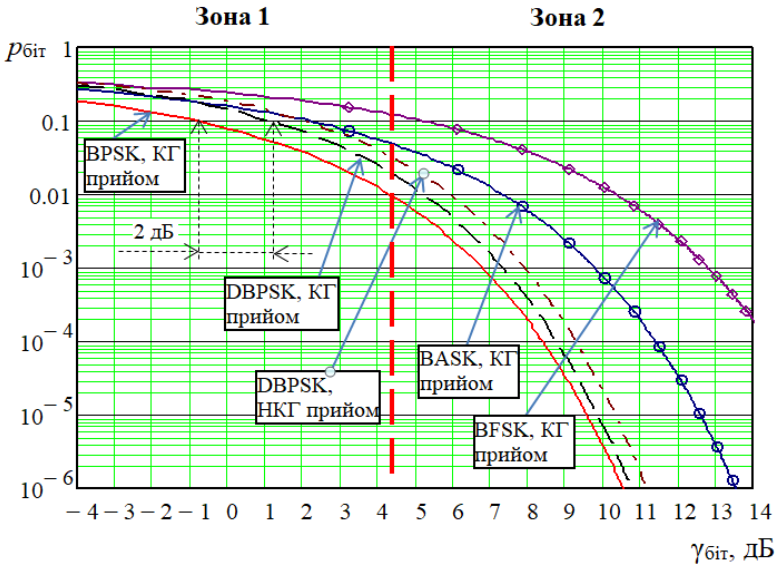

Рис. 1. Ймовірність помилки на біт для сигналів з BPSK, BFSK, BASK, DBPSK при когерентному та некогерентному прийомі

З метою здійснення аналізу завадостійкості сигналів з різними видами фазової маніпуляції в релеєвському каналі було проведено розрахунки за аналітичними виразами, які наведено в [9; 10].

Ймовірність помилки на біт в релеєвському каналі для сигналів з BPSK визначається як:

$$p_{\text{біт}} = \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_b}{\gamma_b + 1}}\right). \tag{4}$$

Ймовірність помилки на біт в релеєвському каналі при КГ прийомі сигналів з DBPSK обчислюється за наступним аналітичним виразом:

$$p_{\text{біт}} = \frac{1}{2} \cdot \left(1 - \frac{4}{\pi}\sqrt{\frac{\gamma_b}{\gamma_b + 1}} \cdot \arctan\sqrt{\frac{\gamma_b}{\gamma_b + 1}}\right). \tag{5}$$

Ймовірність помилки на біт в релеєвському каналі при НКГ прийомі сигналів з DBPSK розраховується за формулою:

$$p_{\text{біт}} = \frac{1}{2\gamma_b + 2}\ . \tag{6}$$

Результати розрахунків за формулами (4)–(6) наведено на рис. 2. З них видно, що перехід від BPSK до DBPSK призводить до погіршення завадостійкості на 2–2,5 дБ. Втрати при переході від КГ DBPSK до НКГ DBPSK є незначними.

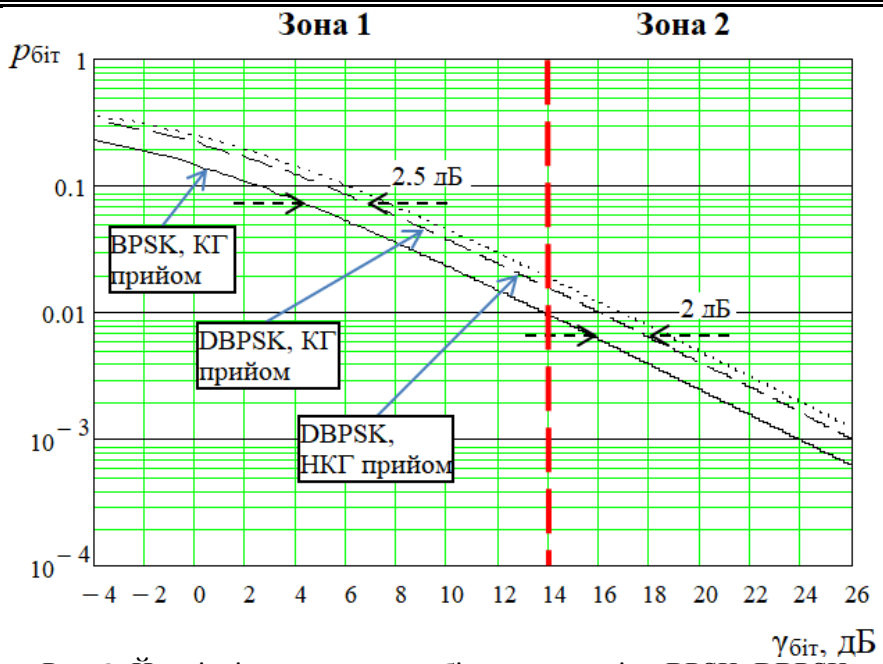

Рис. 2. Ймовірність помилки на біт для сигналів з BPSK, DBPSK при КГ та НКГ прийомі в релеєвському каналі

Оскільки наведені вище технології у більшості випадків використовуються в цивільній сфері, то вибір сигналів з DBPSK маніпуляцією є цілком обґрунтованим, оскільки забезпечує достатній рівень достовірності прийому в каналах, де потужність корисного сигналу значно перевищує потужність шуму (рис. 1 та рис. 2, зона 2).

Сигнали з BPSK дозволяють отримати більшу достовірність прийому при однакових значеннях ВСШ, однак потребують складних схем оцінки фази, які б забезпечили когерентний прийом та мінімізували можливість виникнення явища зворотної роботи [9]. При односторонній радіопередачі в системах спеціального призначення необхідно забезпечити максимально можливу достовірність прийому повідомлень в складній завадовій обстановці (рис. 1 та рис. 2, зона 1), що може бути зумовлена активним впливом засобів РЕБ противника.

Тому одним зі шляхів, що дозволить досягти підвищення достовірності передачі інформації в таких системах, є використання сигналів з BPSK та розв'язання завдань з вдосконалення існуючих схем оцінки фази прийнятого сигналу.

Серед відомих способів підвищення достовірності прийому повідомлень ефективним є завадостійке кодування, але його використання в складній завадовій обстановці, що зумовлена активним впливом засобів РЕБ, є обмеженим, оскільки в таких умовах може призвести до збільшення кількості помилок на етапі декодування (ефект розмноження помилок) [11]. У цьому випадку доцільно використовувати мажоритарний принцип кодування, який дозволяє уникати ефекту розмноження помилок.

Мажоритарний принцип полягає в тому, що в канал посилається непарна кількість разів одного повідомлення, а на приймальній стороні відбувається порівняння між собою однойменних кодових комбінацій (або однойменних двійкових розрядів). На прийомі обирається та кодова комбінація (або біт), яка була прийнята більшу кількість разів [12].

Ймовірність помилкового прийому двійкового символу повідомлення при використанні мажоритарного кодування (порівняння однойменних двійкових розрядів повідомлення, яке повторюється) можна визначити за виразом [12]:

$$p_{\text{бітмаж}} = \sum_{i=\frac{c+1}{2}}^{c} C_c^i \cdot p_{\text{біт0}}^i \cdot \left(1 - p_{\text{біт0}}\right)^{c-i}, \qquad (7)$$

де c – кількість повторів передачі повідомлення або біта;

$p_{\text{біт0}}$ – бітова помилка без використання надлишкового кодування.

Результати розрахунків за формулою (7) для різної міри надлишковості наведено на рис. 3.

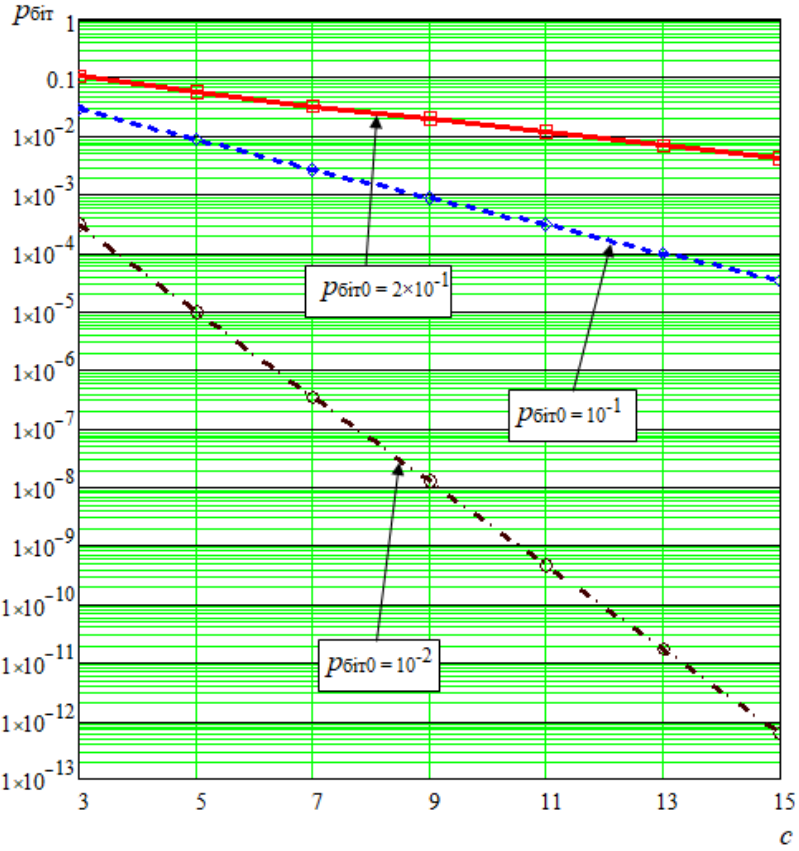

Рис. 3. Залежність $p_{\text{біт}}$ від кратності мажоритарного кодування

Вони свідчать про те, що використання такого способу завадостійкого кодування призводить до підвищення достовірності прийому повідомлень навіть в критичній завадовій обстановці, коли значення бітової помилки в каналі без застосування коригуючих кодів $p_{\text{біт0}} = [2\times10^{-1}; 10^{-1}; 10^{-2}]$.

Недоліком мажоритарного кодування є надлишковість інформації, яка зростає пропорційно кількості повторень одного і того ж повідомлення (біта), тому при його використанні необхідно враховувати часові обмеження на передачу повідомлень.

Варто зазначити, що для систем телеметрії, моніторингу віддалених об'єктів, систем управління БпЛА та інших систем спеціального призначення, крім підвищення достовірності прийому інформації, особливо важливим завданням є забезпечення інформаційної скритності передачі повідомлень. Одним із підходів, що дозволяє розв'язувати такі завдання, є застосування комбінованого випадкового кодування (КВК) [13].

Метод КВК, який запропонований в [13], передбачає використання поєднання завадостійкого кодування і псевдовипадкової зміни ансамблю кодових комбінацій – стохастичного кодування інформації. При цьому висока достовірність передачі повідомлень забезпечується за рахунок завадостійкого кодування, а інформаційна скритність і захищеність від несанкціонованого доступу – за рахунок кодування, що відноситься до некриптографічних методів захисту інформації. При КВК забезпечується теоретико-інформаційний рівень захисту інформації, який визначається рівнем невизначеності вибору ансамблю кодових комбінацій, що відповідають переданому повідомленню, для зловмисника, який здійснює радіоперехоплення [13].

Схема перетворення повідомлень методом КВК наведена на рис. 4 [13].

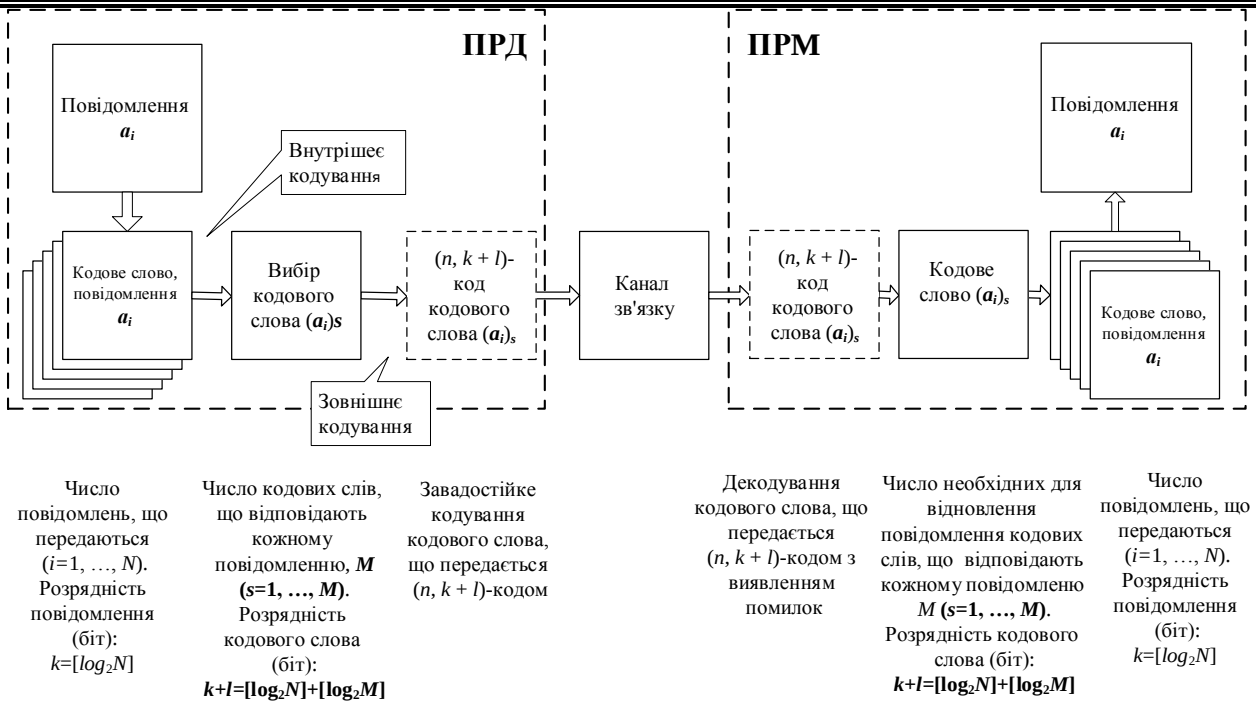

Рис. 4. Схема перетворення повідомлень при їх передачі методом КВК

В цій схемі стохастичне кодування є внутрішнім кодуванням, а завадостійке кодування – зовнішнім. Відповідно, формування кодового слова a_i, $i = 1, \ldots, N$ і його відновлення при прийомі здійснюється в два етапи.

Першим етапом є стохастичне кодування. На цьому етапі, з використанням кодової книги, формується M кодових слів $(a_i)_s$ $s = 1, \ldots, M$, що відповідають повідомленню a_i, і з них за допомогою генератора псевдовипадкових послідовностей (ПВП) вибирається деяке s-те кодове слово. Розрядність вихідного повідомлення a_i відповідає $k = [\log_2 N]$, де $[\cdot]$ означає округлення до найближчого цілого в сторону збільшення, а розрядність кодового слова, що передається $(a_i)_s$, складає $k+l$, де $l = [\log_2 M]$.

Другим етапом формування кодового слова є завадостійке кодування. На цьому етапі здійснюється канальне кодування кодового слова, вибраного з кодової книги, блочним коригуючим (n, k + l)-кодом.

При прийомі повідомлення на першому етапі проводиться декодування прийнятого блочного коду з виправленням помилок і виділення кодового слова $(a_i)_s$, що передавалось. На другому етапі в кодовій книзі вибирається повідомлення a_i, що відповідає виділеному при декодування кодовому слову. Для цього кодові книги в пунктах прийому і передачі повинні бути ідентичними, а для порушника структура кодової книги має бути невідомою.

Підвищення інформаційної скритності при стохастичному кодуванні досягається завдяки використанню книги, в якій кожному повідомленню джерела відповідає набір кодових слів, з яких кодове слово для передачі радіоканалом вибирається випадковим чином, що ускладнює несанкціонований доступ до інформації у випадку радіоперехоплення. Принцип стохастичного кодування на основі кодової книги наведено на рис. 5 [13]. Дискретні повідомлення довжини k, що формуються джерелом, утворюють ансамбль повідомлень a_i, $i = 1, \ldots, N$. Загальна кількість повідомлень (об’єм ансамблю) $N = 2^k$. Кожному повідомленню ставиться у відповідність $M = 2^l$ кодових слів, які зберігаються у визначеному рядку кодової книги і випадковим чином обираються для передавання радіоканалом. Загальне число слів кодової книги $K = MN = 2^{k+l}$. Тоді стохастичний код V може бути представлений як лінійний код, що утворений множиною двійкових послідовностей V_i, $i = 1, \ldots, N$, таких, що $V = \bigcup_{i=1}^{N} V_i$, $V_i \cap V_j = \emptyset$, $i \neq j$. Кожному k-розрядному повідомленню a_i однозначно відповідає одна з підмножин V_i, яка містить M (k+l)-розрядних кодових слів $(a_i)_s$, s = 1, …, M, одне з яких випадково та рівноймовірно вибирається для передачі радіоканалом. Надалі, в процесі зовнішнього завадостійкого

кодування вибране для передачі кодове слово кодується блоковим коригуючим кодом, при цьому загальне число розрядів кодових слів дорівнює $n = k+l+r$.

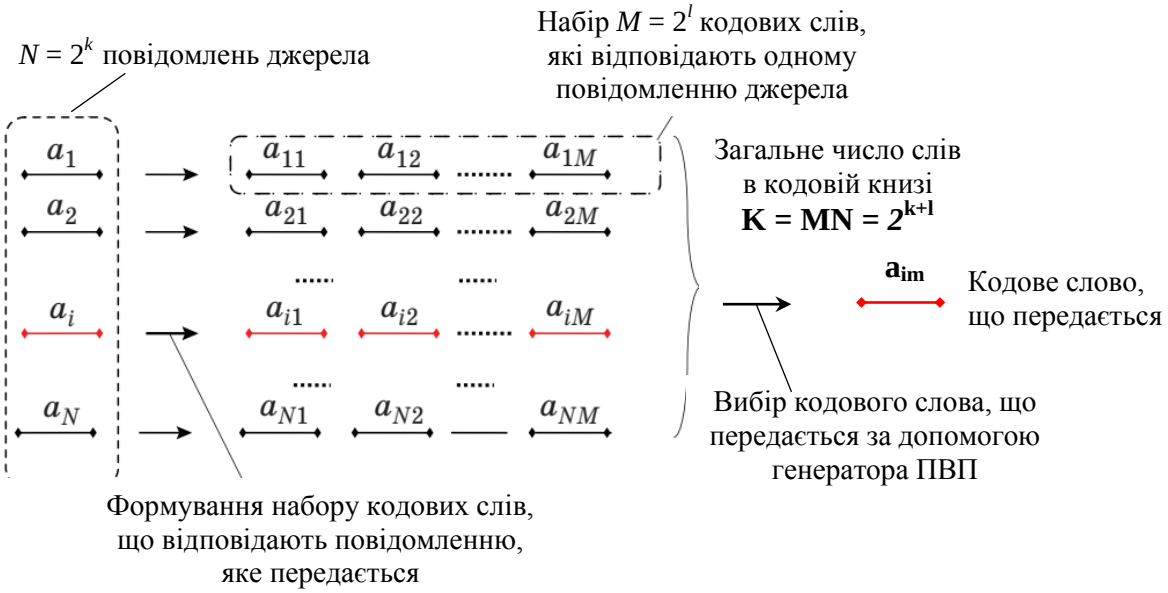

Рис. 5. Принцип стохастичного кодування з використанням кодової книги

Результати досліджень, які отримані в [13], свідчать про те, що застосування стохастичного кодування в поєднанні з завадостійким кодуванням призводить до незначного збільшення ймовірності помилки на біт, але зумовлює зниження швидкості передачі повідомлень в $(n-r)/(n-r-l)$ разів, де n – кількість розрядів повідомлення, r – число перевірочних символів, l – кількість символів стохастичного коду, проте при цьому підвищується інформаційна скритність передачі повідомлень.

В якості кількісної міри інформаційної скритності при стохастичному кодуванні в [13] запропоновано використовувати узагальнений показник рівня інформаційної доступності, який визначається за наступним аналітичним виразом [13]:

$$\delta = \frac{\log_2(Q+1)}{\log_2(M+1)}, \tag{8}$$

де $Q \le 2^t - 1$ – число кодових комбінацій, що правильно виділені зловмисником, $0 \le t \ge l$.

Зрозуміло, що значення Q буде залежати від властивостей конкретних кодів.

В ході проведених досліджень було проаналізовано відомі генератори ПВП, які дозволяють отримувати кодові послідовності для формування кодової книги стохастичного коду.

Тестування генераторів ПВП проводилось за допомогою програми NIST Statistical Test Suite 2.1.2, де використовується пакет статистичних тестів. До його складу входять 188 тестів, метою яких є визначення міри випадковості двійкових послідовностей, згенерованих або апаратними, або програмними генераторами [14].

Досліджувалися стандартизовані генератори двійкових послідовностей, а саме: Linear Congruential Generator (LCG), Quadratic Congruential Generator-I (QCG-I), Quadratic Congruential Generator-II (QCG-II), Cubic Congruential Generator (CCG), Exclusive OR Generator (XORG), Modular Exponentiation Generator (MODEXPG), Blum-Blum-Shub Generator (BBSG), Micali-Schnorr Generator (MSG) та Secure Hash Generator (G-SHA1).

Вихідні дані для здійснення обчислень: довжина послідовностей для тестування $\boldsymbol{n}$ = 387840 біт (мінімально-необхідна довжина послідовності для проведення Universal Statistical тесту); загальна кількість послідовностей $\boldsymbol{m}$ = 1000; рівень значимості $\boldsymbol{\alpha}$ = 0,01; кількість тестів $\boldsymbol{q}$ = 188. Результати обчислень наведено на рис. 6–8.

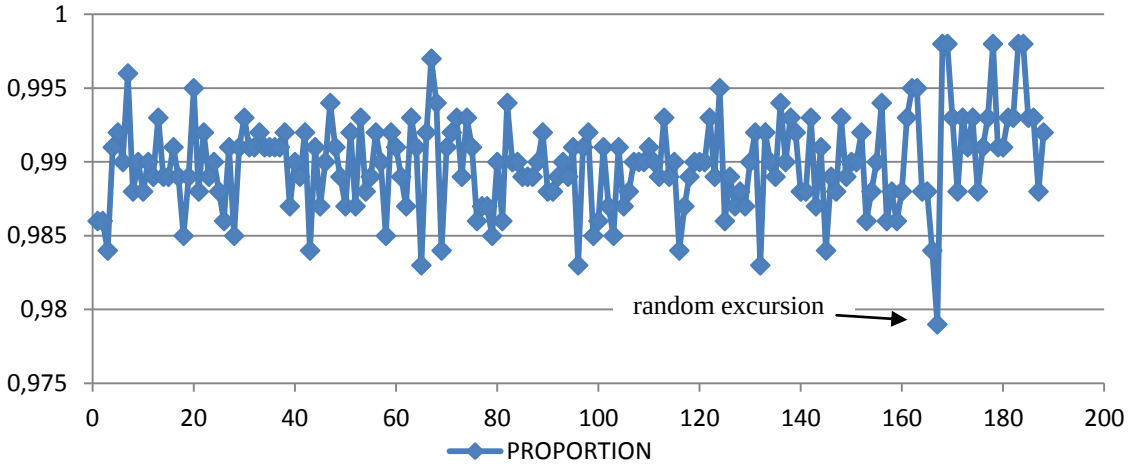

Рис. 6. Micali-Schnorr Generator

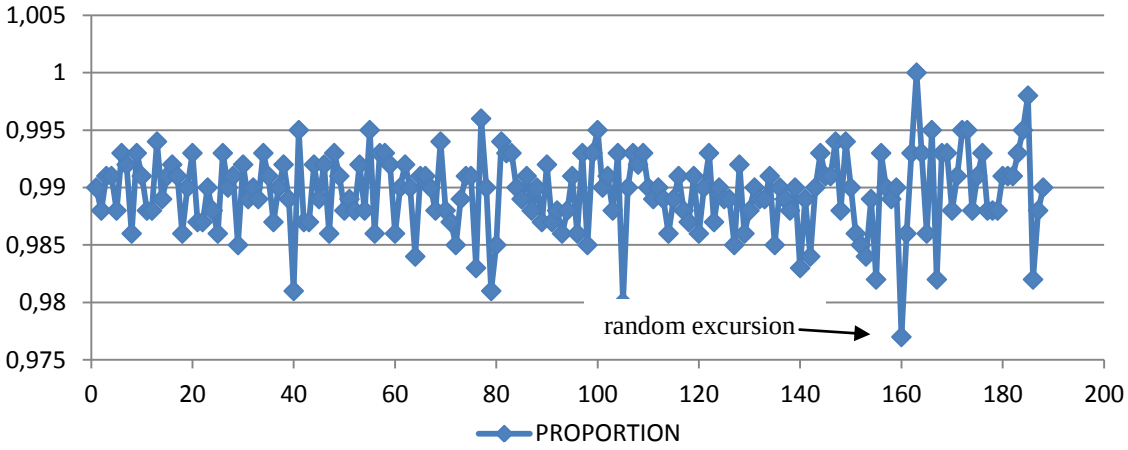

Рис. 7. Linear-Congruential Generator

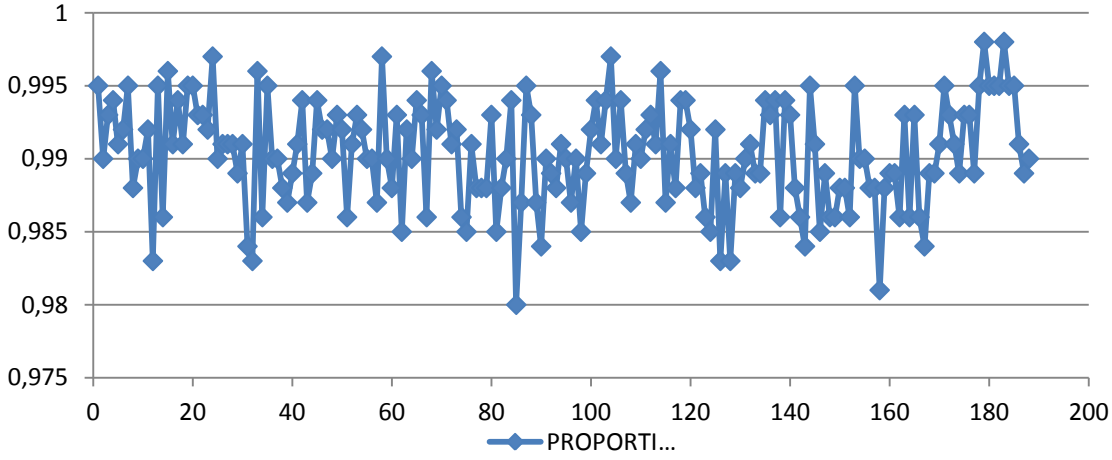

Рис. 8. Blum-Blum-Shub Generator

Відповідно до критеріїв, які визначені в [14], двійкові послідовності, що були згенеровані генераторами LC, BBS та MS, можна вважати такими, що задовольняють сучасним вимогам до ПВП, оскільки більше ніж 98 % із них пройшли всі тести, окрім random excursion (variant) тесту, який пройшли більше ніж 97 % послідовностей.

Висновки. Таким чином, можливими шляхами підвищення достовірності передачі повідомлень односторонніми радіоканалами в сучасних ІКС є вдосконалення існуючих схем оцінки фази прийнятого сигналу та застосування мажоритарного принципу кодування. Перше дозволить використовувати BPSK маніпуляцію, яка порівняно з DBPSK маніпуляцією має

енергетичний виграш до 2 дБ. Виграш по достовірності прийому повідомлень за рахунок мажоритарного кодування залежатиме від обмежень на час передачі інформації.

Крім того, для одночасного підвищення достовірності прийому повідомлень та забезпечення скритності передачі інформації доцільним є застосування принципу КВК. Комбіноване випадкове кодування може здійснюватися як в поєднанні з мажоритарним кодуванням, так і з іншим коригуючим кодом.

Отримані результати досліджень свідчать про те, що для формування кодової книги доцільно використовувати BBS генератори ПВП, оскільки згенеровані ними двійкові послідовності проходять всі тести, що визначені в [14], з найкращими показниками.

У подальших дослідженнях планується розглянути можливість забезпечення криптостійкості кодових конструкцій.

ЛІТЕРАТУРА

1. A Sigfox Energy Consumption Model. Carles Gomez, Juan Carlos Veras, Rafael Vidal, Lluís Casals // Journal Sensors. 2019. Vol. 19. P. 681. URL: https://www.researchgate.net/publication/330947889_A_Sigfox_Energy_Consumption_Model/fulltext/5c5ced9d45851582c3d5a09e/A-Sigfox-Energy-Consumption-Model.pdf.

2. Abbas R., Al-Sherbaz A., Bennecer A., Picton P. A New channel selection algorithm for the Weightless-N Frequency Hopping with lower collision probability. 8th International Network of the Future (NoF) Conference Proceedings. London: IEEE (In Press). 2017. URL: http://nectar.northampton.ac.uk/id/eprint/9777.

3. Ашимов Н. М., Кравцов А. В., Фомин В. В. Надежность управления радиолинии при повторении команд управления на одной частоте. *Спецтехника и связь*. 2009. № 3. С. 38–41.

4. Фрейман В. И. Разработка и исследование моделей систем управления, использующих структурные методы обеспечения помехоустойчивости. *Современные наукоемкие технологии*. 2016. № 8, Часть 1. С. 86–90.

5. Мальцев Г. Н. Чернявский Е. В. Кодирование сообщений в системах радиоуправления без обратного информационного канала. *Информационно-управляющие системы.* 2011. № 4. С. 60.

6. B. Buurman, J. Kamruzzaman, G. Karmakar and S. Islam. *Low-Power Wide-Area Networks: Design Goals, Architecture, Suitability to Use Cases and Research Challenges*. in *IEEE Access.* Vol. 8. P. 17179–17220. 2020. DOI**:** 10.1109/ACCESS.2020.2968057.

7. Bembe, M., Abu-Mahfouz, A., Masonta, M. *A* Survey on low-power wide area networks for IoT applications. *Telecommun Syst* 71, 249–274 (2019). URL: https://doi.org/10.1007/s11235-019-00557-9.

8. Теорія електрозв'язку: підруч. / О. В. Корнєйко, О. В. Кувшинов, О. П. Лежнюк, С. П. Лівенцев; за ред С. П. Лівенцева. Т. 2. Київ: НВП Славутич-Дельфін, 2006. 292 с.

9. Окунев Ю. Б. Цифровая передача информации фазоманипулированными сигналами. Москва: Радио и связь, 1991. 296 с.

10. Лошаков В. А., Лихограй В. Г., Хуссам Дхеа Ал-Джанаби, Таха Насиф Нух. Адаптивная пространственная обработка сигналов в системах LTE С MIMO. *Вісник Національного технічного університету «ХПІ»*. Серія: Нові рішення в сучасних технологіях. 2013. № 11. С. 101–108. http://nbuv.gov.ua/UJRN/vcpinrct_2013_11_17.

11. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: справочник / под. ред. Ю. Б. Зубарева. Москва: Горячая линия-Телеком, 2004. 126 с.

12. Спилкер Дж. Цифровая спутниковая связь / пер. с англ.; под ред. В. В. Маркова. Москва: Связь, 1979. 592 с.

13. Мальцев Г. Н. Помехоустойчивость и скрытность передачи информации по радиоканалам на основе комбинированного случайного кодирования. *Информационно-управляющие системы*, (2), 82-89. https://doi.org/10.15217/issn1684-8853.2015.2.82.

14. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, Version STS-2.1, NIST Special Publication 800-22rev1a, April, 2010. http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

УДК 159.98:004.9:355.2
Кузьменко М. Д. ORCID: 0000-0001-5874-9792 (НМЦ КП МОУ)
Дегтярьов А. С. (НМЦ КП МОУ)
Кіка І. А. (ЗС України)
Кузенков В. С. (ЗС України)

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ОНЛАЙН ПСИХОЛОГІЧНОГО ВИВЧЕННЯ ПЕРСОНАЛУ ЗБРОЙНИХ СИЛ УКРАЇНИ

В умовах сучасного розвитку суспільства значна увага приділяється питанням психологічного вивчення особистості в інтересах забезпечення ефективної діяльності будь-якої організації. Із поширенням у світі інфекції COVID-19 актуалізується необхідність розробки альтернативних передових підходів та механізмів проведення психологічних досліджень. У цьому контексті застосування та впровадження інформаційних технологій та комунікаційних можливостей мережі інтернет вбачається перспективним для організації та проведення психологічного вивчення персоналу. Саме тому ***метою*** *статті є здійснення теоретико-прикладного аналізу сучасних програмно-технологічних рішень щодо онлайн психологічного вивчення персоналу в інтересах Міністерства оборони України та Збройних сил України.*

Проаналізовані існуючі програмно-технологічні рішення, реалізовані через комп'ютерне тестування, такі як системи Moodle, тестова система КТС Net 2, сервіс SURVEY MONKEY, Google Форми тощо. Це допомогло описати загальні спільні риси та характеристики, що висуваються до такого класу програмних рішень. Разом з цим, виявлено й певні прогалини у функціональній складовій існуючих сервісів, що не задовольняють вимогам онлайн психологічного вивчення персоналу Міністерства оборони України та Збройних сил України. Усе це допомогло сформулювати концептуальні вимоги до онлайн-платформи психологічного вивчення персоналу та наблизитися до розроблення сучасного програмного рішення. Комп'ютеризоване онлайн-тестування економить багато часу. Завдання досліджуваного – у зручному форматі надавати відповіді. Отримані дані можуть автоматично фіксуватися, оброблятися, зберігатися та відображатися. Реалізовуються можливість віддаленого тестування та забезпечення конфіденційності результатів.

Ключові слова: *психологічне вивчення, психологічна діагностика, онлайн комп'ютеризоване тестування.*

M. Kuzmenko, A. Degtyarev, I. Kika, V. Kuzenkov Features of organizing and conducting an online psychological study of personnel of the Armed Forces of Ukraine.

In the current progress of society, much attention is paid to the psychological study of personality in the interests of ensuring the effective operation of any organization. With the spread of COVID19 infection in the world, the need to develop alternative best practices and mechanisms for psychological research is becoming more urgent. That is why the use and implementation of information technology and communication capabilities of the Internet is considered promising for the organization and conduct of psychological studies of personnel. That is why the purpose of the article is to carry out theoretical and applied analysis of modern software and technology solutions for online psychological study of personnel in the interests of the Ministry of Defense and the Armed Forces of Ukraine.

Existing software and technology solutions implemented through computer testing, such as the Moodle system, KTC Net 2 test system, Survey Monkey service, Google Forms, etc. are analyzed. This helped to describe the general features and characteristics of this class of software solutions. At the same time, certain gaps in the functional component of the existing services have been identified, which do not meet the requirements of online psychological study of the personnel of the Ministry of Defense and the Armed Forces of Ukraine. All this helped to formulate conceptual requirements for the online platform for psychological study of staff and to get closer to the development of a modern software solution. Computer online testing saves a lot of time. The task of the subject is to provide answers in a convenient format. The received data can be automatically recorded, processed, stored and displayed. The possibility of remote testing and ensuring the confidentiality of results is being implemented.

Keywords: *psychological study, psychological diagnostics, online computerized testing.*

Постановка завдання у загальному вигляді. В умовах сучасного розвитку суспільства значна увага приділяється питанням психологічного вивчення особистості в інтересах забезпечення ефективної діяльності будь-якої організації. Разом з тим, із поширенням у світі інфекції COVID-19 актуалізується необхідність розробки альтернативних передових підходів та механізмів проведення психологічних досліджень. Саме тому застосування та впровадження інформаційних технологій та комунікаційних можливостей мережі інтернет вбачається перспективним для організації та проведення психологічного вивчення персоналу.

Проблеми психологічного вивчення людини, визначення її професійної придатності, професійно-психологічного відбору (далі – ППВ) та психологічної готовності до різних видів діяльності, розроблялися багатьма науковцями як в Україні, так і за її межами. Їх основу

складають дослідження особливостей нервової системи, характерологічних особливостей особистості, психічної діяльності і поведінки. Разом з тим, як свідчить аналіз наукових праць, питання організації та проведення онлайн психологічного вивчення не сьогоднішній день залишається недостатньо вивченим та висвітленим. Відсутність розробленої та впровадженої процедури онлайн психологічного вивчення актуалізує **проблематику** розроблення, впровадження та розгортання сучасних технологічних рішень для вирішення окреслених вище завдань.

Аналіз останніх публікацій. Ретроспективний аналіз стану дослідженості у науковій літературі, проблеми психологічного вивчення людини, визначення її професійної придатності до різних видів діяльності, ППВ, у тому числі й до військової служби, свідчить про те, що її походження має глибоке коріння. На думку сучасних науковців, в цілому поява ППВ значною мірою була обумовлена наявністю двох груп факторів. Перша група пов'язана з намаганнями отримати максимальний прибуток за найменших витратах. Інша – з наявністю певних відмінностей між людьми, які значною мірою визначають ймовірність успішної професійної діяльності в конкретній сфері людської праці.

Проблеми психологічного вивчення досліджували чимало науковців: М. В. Макаренко, М. С. Корольчук, В. В. Кальниш, В. І. Осьодло, Н. Б. Філімонова та інші [3–5; 8; 9]. Перераховані видання присвячені окремим, але дуже важливим проблемам, таким як роль основних властивостей нервової системи і професійних здібностей у розвитку придатності, методичні прийоми психодіагностики, психологічний відбір конкретних спеціалістів тощо.

ППВ військових фахівців організовується та проводиться відповідно до вимог наказу Міністра оборони України від 10.12.2014 № 883 "Про затвердження Інструкції з організації професійно-психологічного відбору у Збройних силах України" та наказом Міністра оборони України від 09.07.2009 № 355 "Про затвердження Інструкції з організації та проведення професійного психологічного відбору кандидатів на навчання у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів", зареєстрованої в Міністерстві юстиції України 22.09.2009 за № 893/16909 [6; 7].

Відповідно до пункту 3 наказу № 883 "основними завданнями професійно-сихологічного відбору особового складу є: *оцінка психологічної та психофізіологічної придатності* військовослужбовців до видів діяльності, до виконання яких вони призначаються, прогноз успішності їх подальшої професійної діяльності під час проходження військової служби та виконання завдань за призначенням; *виявлення осіб з нервово-психічною нестійкістю,* з асоціальними установками та тих, які вживають психоактивні речовини, підготовка та надання керівному складу військових частин (підрозділів) відповідних висновків та рекомендацій; надання рекомендацій з раціонального розподілу особового складу відповідно до рівня розвитку їх *професійно важливих індивідуально-психологічних та психофізіологічних якостей* за військовими спеціальностями." Під час проведення заходів ППВ застосовуються методики та автоматизовані психодіагностичні комплекси (за письмовою згодою) відповідно до переліку психодіагностичних методик, які використовуються під час проведення заходів ППВ у Збройних силах України, затверджених Генеральним штабом Збройних сил України.

Відповідно до пункту 27 наказу Міністерства оборони України № 355 "Про затвердження Інструкції з організації та проведення професійного психологічного відбору кандидатів на навчання у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів" застосовуються методики щодо оцінки мислення, пам'яті, уваги тощо. Варто наголосити, що стимульний матеріал тестових методик є досить різноманітним: тестові завдання можуть варіюватися від текстового формату до мультимедійного; варіанти відповідей – від дихотомічних до відкритих; завдання можуть мати обмеження в часі або вимагати фіксації часу виконання окремих завдань. Передбачено також застосування й спеціалізованих приладів для вирішення завдань ППВ.

Відповідно до наказів науково-методичне та програмне забезпечення здійснюють Національний університет оборони України імені Івана Черняховського, Українська військово-медична академія, Головне управління морально-психологічного забезпечення Збройних сил України, науково-дослідні установи Збройних сил України, що в свою чергу актуалізує

необхідність розроблення сучасних програмних рішень для підвищення ефективності заходів психологічного вивчення персоналу та унормування застосування відповідної процедури. **Метою** статті є здійснення теоретико-прикладного аналізу сучасних програмно-технологічних рішень щодо онлайн психологічного вивчення персоналу в інтересах Міністерства оборони України та Збройних сил України.

Виклад основного матеріалу дослідження. Активність заходів психологічного вивчення полягає також і в тому, що їхнє проведення не має обмежуватися констатацією "діагнозу" або "прогнозу" і у випадку несприятливих висновків результати психологічного обстеження варто використовувати для рекомендації з корекції професійних планів, орієнтації на більш адекватні професійні вибори. Цей принцип означає можливість за результатами обстеження вирішувати завдання раціонального розподілу фахівців, обґрунтувати рекомендації з розвитку недостатньо виражених професійно-важливих якостей та індивідуалізувати процес навчальної і трудової діяльності тощо [4].

Проведення заходів психологічного вивчення передбачає психологічне діагностування (вимірювання) властивостей особистості. Психодіагностика як теоретична дисципліна розглядає закономірності винесення валідних і надійних діагностичних суджень, за допомогою яких здійснюється перехід від ознак, або індикаторів, певних психічних якостей, структур, станів або процесів до наявності й/або вираженості цих психологічних змінних в об'єкта дослідження. Практичним завданням психодіагностики є розробка методів реєстрації психічних якостей, індикаторів, перевірка надійності й валідності існуючих методик, створення процедур інтерпретації одержуваних даних.

Удосконалення ППВ та психологічного вивчення персоналу обумовлене багатьма організаційними, методологічними й практичними факторами, серед яких:

– необхідність врахування нових принципів структури ЗС України, строків служби відповідних категорій особового складу;

– ускладнення й підвищення екстремальності професійної діяльності військових фахівців в цілому;

– необхідність відновлення організаційної й методичної бази системи ППВ військових фахівців.

Особливо популярним останнім часом стає *комп'ютеризоване тестування,* яке порівняно з традиційним (бланковим) тестуванням має ряд переваг: отримання миттєвого результату, виняток упередженості, легкість обробки результатів й ін. Основні труднощі, з якими доводиться стикатися при порівняльній оцінці систем тестування, – це визначення критеріїв для порівняльних оцінок інформаційних систем. Пропонується аналіз особливостей інформаційних систем тестування за наступними показниками: складність роботи з програмою розробника тестів; функціональні можливості, пов'язані з організацією тестування (можливість проведення тестування у мережі, підтримка різних типів запитань тощо). Функціональні можливості пов'язані з обробкою і представленням результатів (ведення статистики, висновок на екран дослідника поставлених запитань і відповідей користувача й ін.) [2, с. 26].

Комп'ютеризоване тестування має низку незаперечних переваг перед іншими його формами, що обумовлено наступними обставинами:

- можливість застосуванням різних видів наочності (малюнки, відеофрагменти, комп'ютерні моделі тощо);
- комп'ютер більше, ніж присутність експериментатора, спонукає досліджуваного до самостійності, звідси – вище діагностична цінність результатів;
- можна судити про індивідуальні особливості стратегії діяльності випробуваного, оскільки знижується вплив особистісних особливостей експериментатора і випадкових поведінкових факторів на стратегію;
- з'являється можливість порівняти експериментальні дані, отримані різними дослідниками;
- автоматизується складна обробка даних, з'являється можливість швидко отримати порівняльні результати за великими масивами даних, зберігати і порівнювати їх;
- з'являється можливість застосовувати такі форми, як імітаційні вправи, аналіз ситуацій;

- можливо включати у сферу тестування елементи психодіагностики, установок, почуттів, вражень, впливу когнітивних стилів;
- можливо використовувати адаптивну стратегію тестування, коли стратегія дослідження змінюється залежно від отриманих раніше результатів [2].

Обираючи програмне забезпечення для вирішення завдань тестування, важливо також визначити, чи будуть тестові завдання однорідними за складністю, чи слід передбачити можливість зміни порядку їх подання на сусідніх комп'ютерах в аудиторії, де проводиться тестування, чи потрібно обмежувати час на виконання тестового завдання, чи є можливість зміни шкали оцінювання експертом.

У Збройних силах України для здійснення психологічного вивчення на правах рекомендаційного характеру функціонують програмні комплекси "СПД-ЛІДЕР", "АРМ-ПСИХОЛОГ", "ЯШМА", "ЕФЕС", "PSY-D" та інші. Проте жодна з цих платформ не реалізує можливості саме віддаленого онлайн-тестування особового складу

Онлайн психологічне вивчення вже реалізовується в освітньому процесі. Для удосконалення процесу навчання і освіти, підвищення успішності, раціонального розподілу навчального навантаження необхідно проводити моніторинг психічного стану учнів освітніх установ середньої та вищої професійної освіти з метою виявлення причин низького засвоєння знань, оцінки інтелектуального розвитку, виявлення проблем адаптації в колективі, а також вирішення проблеми профорієнтації. Найбільш поширена форма такого моніторингу – психологічне тестування, що являє собою метод вимірювання та оцінки психологічних характеристик людини за допомогою спеціальних технік [1]. Перспективним напрямком в цій галузі є розвиток і використання онлайн-тестування, яке дозволяє істотно скоротити витрати часу на збір і обробку результатів, мінімізувати помилки в процесі обробки результатів, а також поширити досвід роботи психологів вищої кваліфікації за рахунок комп'ютерної інтерпретації результатів тестування.

В освітньому середовищі неабиякого поширення набула підсистема тестування системи Moodle:

1. Дозволяє за допомогою стандартних засобів (редакторів, web-форм і под.) швидко і просто створити повноцінний комплект тестових матеріалів з можливістю редагування і управління ним у реальному масштабі часу.

2. Дозволяє працювати з системою з різних місць (локально і дистанційно, з навчального класу, з робочого місця або з дому); підтримує кілька типів питань в тестових завданнях (множинний вибір, на відповідність, вірно/невірно, короткі відповіді, есе та ін.); надає можливість встановлення шкали оцінки, існує механізм напівавтоматичного перерахунку результатів; в системі містяться розвинені засоби статистичного аналізу результатів тестування.

3. Після тестування формується таблиця з оцінками респондентів (аналіз відповідей дозволяє з'ясувати, при відповіді на які питання було найбільше помилок).

Тестова система *KTC Net 2:* дозволяє створювати і редагувати тести різної спрямованості і складності, практично не висуваючи особливих вимог до користувача, за винятком наявності базових навиків поводження з персональним комп'ютером та офісними програмами; забезпечує можливість проведення тестування у мережі, забезпечення захисту інформації паролем і стиснення інформації всередині підсумкового файлу тесту для компактного зберігання; можливість створення тестових завдань закритого та відкритого типу; підтримка різних типів запитань, забезпечення індивідуального налаштування пріоритетів для кожного питання і варіанти відповіді й ін.; виводить статистику з підтримкою сортування, експортом в текстові файли та файли електронних таблиць.

Сервіс *SURVEY MONKEY* призначений для створення швидких онлайн-опитувань. У безкоштовному тарифі передбачено до 10 питань для 1 анкети і робота зі 100 респондентами. Підходить для великих компаній, оскільки програма гарантує високий рівень контролю та безпеку під час керування даними. Може використовуватися для організації наради, опитування покупців, анкетування учасників заходу. Доступниий також мобільний додаток. У платформі доступні графіки з докладними звітами. Сервіс містить інструменти для спільної роботи, створення тестів з виставленням оцінки, можливості для брендингу анкети. Отримані відповіді

можна експортувати у файлові формати .pdf, .xls, .csv, .ppt. Доступна інтеграція з MailChimp. Плюси: можливості для настройки брендингу; аналітика опитувань; A/B-тестування; перегляд даних під час анкетування. Мінуси: відсутня можливість вставляти файли в питання. Вартість: безкоштовний тариф (до 10 питань).

Google Форми є різновидом хмарного сервісу – певне сховище даних, в якому вони зберігаються на певних серверах, які надають право в користуванні. Google Форми – це зручний інструмент, за допомогою якого можна легко і швидко планувати, складати опитування, анкети, тести та вікторини, а також збирати іншу інформацію. Посилання для заповнення форми (для відповідей на запитання тесту, анкети тощо) можна надсилати електронною поштою. Google Форми дають широкий спектр можливостей використання у навчальному та науковому процесі та полегшують роботу при підготовці завдань: зникають паперові версії питань (дані про опитування можуть зберігатися в електронному вигляді). Основна робота з Google Формами полягає у додаванні питань. Крім питань, сервіс дає змогу додавати зображення та відео з Youtube. Особливістю сервісу є те, що після заповнення запропонованих форм вся інформація в автоматичному режимі акумулюється у спеціальних таблицях і обробляється, що дає змогу отримати звіт із відповідними діаграмами. Це полегшує роботу педагога і дозволяє скоротити час для обробки даних та їх систематизації.

Google Форми застосовують не тільки для мініопитувань і голосувань, але й у великих дослідженнях, де кількість питань може обчислюватися десятками. За допомогою цієї програми можна зробити тестові завдання більш вдало та якісно. Можливість завантажити програму на телефон або планшет дає змогу застосовувати форми будь-де. В системі передбачені різні шаблони оформлення, а також можливість завантаження свого логотипу та фото. На вибір пропонується кілька дизайнів питань: вибір відповіді, поля тексту, ускладнені сітки введення. Можна створити багаторівневе опитування, тоді учасник буде переходити на інші сторінки залежно від своїх відповідей. Додаток дозволяє використовувати додаткові плагіни. До плюсів можна віднести: необмежену кількість анкет; висновок результатів у вигляді графіків; вивантаження відповідей в таблицю Google; різні теми оформлення. Мінуси: відсутність автоматичної обробки опитування; відсутність можливості вставити на сайт. Вартість – безкоштовний сервіс.

З метою організації процедури онлайн психологічного вивчення персоналу Збройних сил України необхідно розробити зміни до існуючих нормативно-правових документів та розробити спеціалізоване програмне забезпечення, яке б відповідало потребам замовника. Програмне забезпечення повинно являти собою конструктор інструментарію психологічного вивчення і мати підсистеми "адміністратора", "дослідника" "клієнта".

Загальні вимоги до "Вебплатформи" можуть бути такі:

запитання (стимули) можуть бути текстовими, графічними, мультимедійними, посиланнями та варіативними формами відповіді – дискретними варіантами, відкритими відповідями; варіант (варіанти) можуть обиратися шляхом встановлення знаку навпроти;

запитання (стимули) повинні мати назву та текстовий опис, можуть бути оціненими за шкалою від 0 (1) до 10 у різних варіаціях; мати підписи під кожним варіантом відповіді на вибір адміністратора;

запитання (стимули) можуть бути обов'язковими або факультативними, перехід від одного до іншого може бути лінійним або за умови виконання правила;

клієнтська підсистема повинна забезпечувати доступ до проходження окремого дослідження (в тому числі бути адаптована до можливостей сучасних мобільних пристроїв – смартфонів);

порядок доступу визначає адміністратор (генерування перманентного посилання, надання логіна та пароля тощо);

вебплатформа повинна мати можливість функціонувати безперервно у режимі «08:00–19:00» (сім днів на тиждень).

обмін даними між пристроями Клієнтів та вебсервером здійснюється за допомогою мережі Інтернет;

інформаційний обмін між вебсервером та сервером результатів досліджень повинен здійснюватися внутрішніми мережами ЗС України;

інформаційне забезпечення має забезпечувати зберігання даних у вигляді, що дозволяє організувати роботу з системою для багатьох користувачів, розподіл і надання прав доступу на основі системних ролей; роботу користувачів підсистеми з інформаційними ресурсами в режимі реального часу.

Висновки. Зважаючи на проаналізований досвід організації психологічного вивчення, професійно-психологічного відбору, можна дійти висновку, що наразі є недоступним вирішення завдань онлайн психологічного вивчення, яке б задовольнило потреби Збройних сил України повною мірою.

Саме тому перспективним вважається розроблення вебплатформи онлайн психологічного вивчення персоналу, це має багато суттєвих переваг: часових, організаційних, ресурсних, методичних тощо. Вирішення організаційно-адміністративних завдань забезпечення процедури вплине на розроблення вимог та відповідної методичної документації для всебічного забезпечення онлайн психологічного вивчення в інтересах Збройних сил України.

Напрямками подальших досліджень вважається реалізація розроблених технічних вимог у програмному рішенні, апробація й отримання досвіду дослідної експлуатації програмного забезпечення для вдосконалення та забезпечення стабільної роботи.

ЛІТЕРАТУРА

1. Белов С. В., Техтилова А. В. Автоматизированная система психологического тестирования учащихся средних и высших учебных заведений. *Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.* 2016. № 1. С. 116–124.

2. Ефимов Е. Н., Денисов М. Ю., Жилина Е. В. Сравнительный анализ образовательных систем тестирования по критерию функциональной полноты. *Управление экономическими системами:* электронный жур-л. 2012. № 4. URL: http://www.uecs.ru.

3. Корольчук М. С. Актуальні проблеми психофізіології професійної діяльності військових спеціалістів. Київ: КВГІ, 1996. 144 с.

4. Корольчук М. С., Крайнюк В. М. Теорія і практика професійно-психологічного відбору: навч. посіб. для студентів вищих навчальних закладів. Київ: Ніка-Центр, 2006. 536 с.

5. Макаренко Н. В. Теоретические основы и методики профессионального психологического отбора военных специалистов. Київ: "Сент-Жак", 1996. 336 с.

6. Про затвердження Інструкції з організації професійно-психологічного відбору у Збройних Силах України: наказ Міністра оборони України від 10.12.2014 № 883. URL: https://zakon.rada.gov.ua/laws/show/z0013-15.

7. Про затвердження Інструкції з організації та проведення професійного психологічного відбору кандидатів на навчання у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів: наказ Міністра оборони України від 09.07.2009 № 355. URL: https://zakon.rada.gov.ua/go/z0893-09.

8. Осьодло В. І. Сучасний стан і перспективи психологічного забезпечення в Збройних силах України. URL: http://chasopys-ppp.dp.ua /index.php/chasopys/article/download/37/34.

9. Shymko V. A. Using Phenotypology Hypotheses as a Personality Assessment Tool: the Tentative Validation Study. *PSYCHOLOGICAL JOURNAL*. № 5. Vol. 6. Pp. 9–17. URL: https://www.apsijournal.com/index.php/psyjournal/article/download/957/574.

10. Філімонова Н. Б. Факторний аналіз мікроструктури оперативної пам'яті на зорові вербальні та невербальні стимули у чоловіків та жінок / Н. Б. Філімонова, Т. В. Куценко // Ученые записки Таврического национального университета им. В. И. Вернадского. Серия «Биология, химия». Том 22 (61). 2009. № 2. С. 134–139.

УДК 004.85 Любарський С. В. ORCID: 0000-0001-8068-1106 (ВІТІ)

ПІДХІД У РЕАЛІЗАЦІЇ МОДЕЛІ ОБЛІКУ ЗБИТКУ ТА КОНТРОЛЮ ВІДНОВЛЕННЯ ЗРУЙНОВАНОГО В РЕЗУЛЬТАТІ РОСІЙСЬКОЇ АГРЕСІЇ НЕРУХОМОГО МАЙНА МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ НА ОСНОВІ СТАТИСТИЧНО-АНАЛІТИЧНОЇ ОБРОБКИ ДАНИХ

Концепція розвитку цифрової економіки та суспільства України ключовим напрямком ставить розвиток цифрової інфраструктури держави. Особливо актуальним виступає цифровізація процесів підтримки прийняття рішень у сфері діяльності силових відомств України. Актуальність цифровізації процесів обліку руйнації об'єктів нерухомого майна Міністерства оборони України саме обумовлена умовами військового стану і характером ведення бойових дій.

Запропонована архітектура інформаційно-аналітичної системи спрямована не тільки реалізувати функціональності з обліку ступеню руйнації споруд і комунікацій Міністерства оборони України, але і надати зручний прикладний інтерфейс експертам з точки зору виробітку кваліфікованих експертних рішень у відновленні ситуації в стислі терміни часу.

Головним елементом інформаційно-аналітичної системи виступає підсистема інформаційно-аналітичної підтримки прийняття рішень, яка формує статистично-аналітичні дані по всіх об'єктах МОУ та ЗСУ та здійснює прогноз на обсяг відновлювальних робіт по об'єкту руйнації (ремонт/реконструкція).

Вдосконалення процесів обробки статистично-аналітичних даних і підвищення ефективності формування кваліфікованих рішень пропонується здійснювати на основі методів Machine Learning.

Ключові слова: *діджиталізація, облік нерухомого майна, інформаційно-аналітична система, статистично-аналітичні дані, методи Machine Learning.*

S. Liubarskyi An approach to the implementation of the damage accounting model and control over the restoration of real estate destroyed as a result of russian aggression of the Ministry of Defense of Ukraine based on statistical and analytical data processing

The concept of development of the digital economy and society of Ukraine puts the development of the digital infrastructure of the state in a key direction. The digitalization of decision-making support processes in the sphere of activity of law enforcement agencies of Ukraine is especially relevant. The urgency of digitalization of the processes of accounting for the destruction of real estate of the Ministry of Defense of Ukraine is due to the conditions of martial law and the nature of hostilities.

The proposed architecture of the information-analytical system is aimed not only to implement the functionality of accounting for the degree of destruction of buildings and communications Ministry of Defence, but also to provide a user-friendly interface to experts in terms of developing qualified expert decisions to restore the situation in a short time.

The main element of the information-analytical system is the subsystem of information-analytical decision-making support, which generates statistical and analytical data on all objects of Ministry of Defence and forecasts the volume of restoration work on the object of destruction (repair / reconstruction). It is proposed to improve the processes of statistical and analytical data processing and increase the efficiency of forming qualified solutions on the basis of Machine Learning methods.

Keywords: *digitalization, real estate accounting, information-analytical system, statistical-analytical data, Machine Learning methods.*

Постановка завдання. На поточний момент часу внаслідок російської агресії загальна площа зруйнованого або пошкодженого житла в Україні наразі складає 9,401 млн кв. м. Запуск процесу компенсації і відновлення такого житла планується вже незабаром, не чекаючи на міжнародні суди та отримання репарацій. До остаточного ухвалення Верховною Радою законопроєкту № 7198 "Про компенсацію за пошкодження та знищення окремих категорій об'єктів нерухомого майна внаслідок бойових дій, терористичних актів, диверсій, спричинених військовою агресією російської федерації" питання фіксації збитків регулюється нормативно-правовими актами Кабінету Міністрів України. Передовсім постановами "Про затвердження Порядку визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації" від 20 березня 2022 р. № 326 та "Про збір, обробку та облік інформації про пошкоджене та знищене нерухоме майно внаслідок бойових дій, терористичних актів, диверсій, спричинених військовою агресією російської федерації" від 26 березня 2022 р. № 380. Документами, поміж іншого, визначено основні показники, які враховуватимуть при оцінюванні заподіяної шкоди. В першу чергу – фактичні витрати на відновлення пошкодженого житлового фонду і об'єктів інфраструктури, фактичні витрати на грошову компенсацію

постраждалій стороні, вартість зруйнованого та пошкодженого житла, яке потребує відновлення. Інфраструктура, яка належить Міністерству оборони України (МОУ), з цього приводу – не виняток. Президентом України визначено напрямок на "діджиталізацію", а саме оцифрування всіх можливих процесів в державних структурах, в тому числі контролю якості виконання робіт щодо будівництва, реставрації, відновлення та технічного обслуговування об'єктів нерухомого майна МОУ, що, в свою чергу, спростить низку адміністративних процесів, зменшить бюрократичну складову та допоможе у швидкому відновленні країни.

Для оцінки збитків, які нанесено об'єктам житлового та нежитлового фонду МОУ, та прийняття раціонального рішення щодо їх подальшої експлуатації (будівництво, реконструкція, технічне переоснащення, реставрація, капітальний ремонт) в квартирно-експлуатаційних органах МОУ можуть бути задіяні наступні документи [1; 2]:

- індивідуальна картка обліку будівлі;
- зведена картка обліку наявності та якісного стану будівель;
- індивідуальна картка обліку земельної ділянки;
- індивідуальна картка обліку системи теплопостачання;
- зведена картка обліку систем теплопостачання;
- індивідуальна картка обліку системи газопостачання;
- індивідуальна картка обліку газового обладнання будівлі;
- зведена картка обліку систем газопостачання.

Слід відзначити, що ведення вищезазначених форм ведеться даними підрозділами вручну і зберігається в архівах в паперовому вигляді з дублюванням інформації у файлових архівах виконавців в *Excel*-форматах.

Незважаючи на застарілість способів ведення обліку нерухомого майна в Збройних силах України (ЗСУ), керівництво та особовий склад здійснювали спроби автоматизувати процес обліку. Прикладом може слугувати ведення таблиць нерухомих об'єктів МОУ співробітниками ГКЕУ МОУ у *Microsoft Excel*, які синхронізовані зі спеціальною табличною формою, яка використовується в армії США. Таблична форма використовується для введення нових звітних даних нерухомого майна МОУ та відображення вже збережених звітів. *Excel*-таблиця використовується як сховище, де знаходяться всі збережені дані по звітах про стан робіт на об'єктах МОУ.

Крім того, для обліку також використовували програмне забезпечення *FoxPro*, де певною мірою спрощена процедура обліку нерухомого майна ЗСУ. Додаток *FoxPro* оперує даними по обліку нерухомого майна МОУ згідно з формою 40.

Отже, можна зробити висновок, що для виконання завдань обліку збитку та контролю відновлення нерухомого майна МОУ на всіх його етапах виконавцями задіяні різні інструментальні засоби, що зберігають дані в різних, іноді несумісних для міграції даних між підрозділами, форматах. Також слід відзначити, що кожний об'єкт нерухомості характеризується величезною групою параметрів, що носять як кількісний, так і якісний характер. Деякі з об'єктів знаходяться в зоні окупації і зробити їх якісну оцінку стану не можливо. Немає змоги у стислі терміни часу об'єктивно оцінювати ситуацію по вибірково обраним категоріям об'єктів (район, місто, регіон, лінія бойового зіткнення, довільний полігон місцевості тощо).

Тому, до задачі діджиталізації у даній предметній області слід віднести наступні функціональні процеси:

- організацію процедури моніторингу стану руйнації об'єктів житлового та нежитлового фонду МОУ на основі встановлених керівними документами експлуатаційно-технічних показників;
- формалізацію і збереження інформації, що отримана від процедури низового моніторингу у вигляді єдиного сховища даних за умови обов'язкової процедури валідації прийнятих даних;
- оперативне отримання інформації про всі об'єкти нерухомого майна, що перебувають на обліку МОУ (найменування будівельної споруди, розташування об'єкта за геолокацією, найменування та номер військової частини, найменування структурного підрозділу ЗСУ, до

якого прив'язується споруда, гарнізон, стан об'єкта (споруди): ступінь руйнації та рівень його готовності для використання за призначенням тощо) у вигляді, що забезпечує їх якісну інтерпретацію в контурах підтримки прийняття рішень. Надання змоги перегляду об'єктів нерухомого майна на цифровій мапі України з прив'язкою до геопросторових даних;

– редагування формалізованих даних за відповідною предметною областю на підставі адміністративних прав та повноважень. Унеможливлення фальсифікації провалідованих даних;

– забезпечення непротисуперечності, надійності та безпеки даних на рівні програмної логіки розподіленої інформаційної системи та на рівні комунікаційних з'єднань;

– формування статистично-аналітичних даних (САД) по об'єктах МОУ з візуалізацією їх в прикладних інтерфейсах і подальшим прогнозування можливості вчасного завершення робіт над об'єктами, які підляглися руйнації;

– формування звітів статистично-аналітичної діяльності за визначеними критеріями з можливістю подальшого документування. Застосування для звітних даних форматів, що найбільш застосовані у роботі корпоративних систем.

Вищезазначені процеси слід інтегрувати в логіку роботи інформаційно-аналітичної системи спеціального призначення; архітектуру, функціональність і важелі, що суттєво вплинуть на якість приймаємих рішень, розглянемо детальніше.

Аналіз останніх публікацій щодо вирішення проблем по автоматизації процесів обліку та контролю нерухомого майна в силових структурах країн-членів НАТО свідчить про пріоритетність впровадження в сучасні інтегровані програмні платформи підтримки прийняття рішень наступних процесуальних напрямків:

– урахування вимог будівельної галузі з перевіреними найкращими практиками. Ідеальна для впровадження нових бізнес-моделей в міру розвитку ринку;

– реформація бізнес-процесів за допомогою інтелектуальної автоматизації;

– пришвидшення прийняття рішень за допомогою вбудованої аналітики, голосового інтерфейсу та цифрових помічників;

– оцифрування процесів за допомогою гібридних, хмарних та локальних сценаріїв, які містять послідовну модель даних, вихідний код та зручний користувальницький досвід.

Метою статті є пропозиція у підвищенні ефективності прийняття оптимальних рішень у сфері будівництва, реставрації, відновленні, технічного обслуговування об'єктів нерухомого майна МОУ під час воєнного стану завдяки діджиталізаці процесів збору даних про об'єкти руйнації, які належать МОУ, вдосконалення процесів аналізу цих даних методами машинного навчання та визначення об'єктивної експертної оцінки ступеня руйнації.

Цільова настанова обумовлює виконання наступних завдань:

– аналіз особливостей обліку збитків нерухомого майна в МОУ за умов військового протистояння;

– обгрунтування вибору раціональної моделі архітектурної реалізації інтеграційної інформаційно-аналітичної системи підтримки прийняття рішення (СППР), будови та функціонального навантаження її підсистем та модулів;

– обґрунтування місця та ролі процесів обробки статистично-аналітичних даних в загальній архітектурній будові інформаційної системи;

– вдосконалення процесів обробки статистично-аналітичних даних і підвищення ефективності відповідних задач за рахунок впровадження методів *Machine Learning* (*ML*).

Виклад основного матеріалу. На сьогоднішній день можна констатувати майже повну відсутність комплексної автоматизації процесів обліку процесів логістики в МОУ, особливо обліку нерухомого майна. Відділи, на які покладено виконання подібних задач, продовжують використовувати застарілі методи контролю та обліку, друкуючи звіти на паперових носіях, що ускладнює, затримує та не раціоналізує увесь процес обліку нерухомого майна. Військовий стан, стислість термінів на прийняття рішень, існуючі методи роботи співробітників відповідних служб, унеможливлення зробити експертну оцінку руйнувань на окупованій території – всі ці фактори суттєво обмежують ефективне вирішення задачі, аналіз ступеня збитку і підготовки адекватного реагування.

Досвід впровадження засобів електронного обліку будівництва об'єктів Міністерства оборони країн-членів НАТО обумовлює необхідність діджиталізації наступних інформаційних процесів, які об'єктивно повинні бути враховані в моделі інформаційно-довідкової системи:

– автоматизований збір даних, що передбачає виключення трудомісткості та фактору операторної помилки;

– структурування стандартних даних, зібраних з різних джерел. Дані структурування гарантують, що інформацію можна вводити один раз, а потім використовувати багато разів у кількох місцях, без погіршення якості та додаткового навантаження;

– управління інформаційним ризиком (захисту від можливого зловживання інформацією про об'єкти);

– аналітична можливість (визначення аномалій, відстеження та аналіз тенденцій розвитку процесів, оцінка ефективності будівельних або монтажних проєктів).

Зазначені процеси інтегровані в архітектуру таких інформаційних систем, як *MilCon Dashboard* [3], *RMS* [4].

На рисунку 1 зображено архітектурну будову інформаційно-аналітичної системи *MilCon Dashboard* (США).

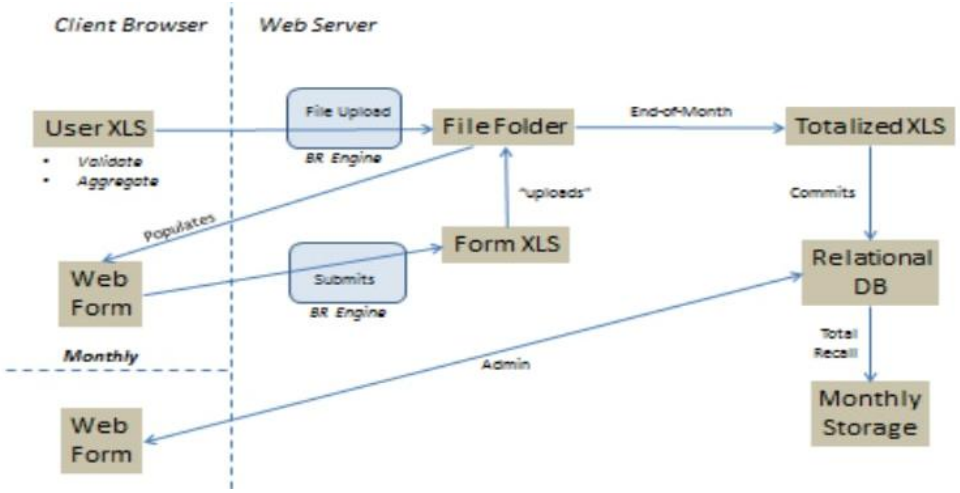

Рис. 1. Архітектура *MilCon Dashboard*

Клієнтська частина архітектури надає змогу переглядати та вносити щомісячні звіти через вебформу прикладного інтерфейсу. Серверна частина складається з: компоненту обробки щомісячних звітів; підтвердження звітів та збереження до реляційної бази даних. Архітектура передбачає: автоматизований збір даних; структурування даних, зібраних з різних джерел; управління інформаційним ризиком; вдосконалені аналітичні можливості. На інформаційній панелі *MilCon* зберігатимуться вичерпні, перевірені, стандартні дані проєкту, а кінцеві користувачі зможуть генерувати впорядковані та динамічні запити на основі інформації майже у реальному часі. Ця розширена аналітична можливість дозволяє фахівцям *MilCon* зрозуміти виконання будівництва об'єктів, визначити аномалії, відстежувати та аналізувати тенденції, оцінювати ефективність будівельних або монтажних проєктів та визначати ефективні можливості економії [3].

Але архітектурна реалізація не позбавлена певних обмежень відносно предметної області, яка винесена на дослідження:

– система орієнтована на облік нерухомого фонду міністерства у мирний час;

– Міністерство оборони США збирає велику кількість даних, пов'язаних із будівництвом, але йому не вистачає стандартизованих процесів та інтегрованих систем, необхідних для систематичного відстеження, аналізу та звітності про проєкти військового будівництва та пов'язаних з ними витрат. Далі, інформацією щодо покращення ефективності військового будівництва в даний час керують лише настільки, наскільки це потрібно для зовнішньої звітності.

Основним інструментом контролю електронного банку Міністерства оборони Сполученого Королівства Великої Британії та Північної Ірландії є програмне забезпечення для контролю житловим майном – *RMS* [4].

RMS пропонує повнофункціональну систему управління майном, пристосовану до конкретних потреб військових. *RMS* інтегрований у військових управліннях по всій Великобританії та забезпечує вдосконалене рішення щодо менеджменту нерухомою власністю, квартирами, об’єктами Міністерства тощо.

RMS забезпечує унікальний та зручний користувальницький інтерфейс, який легко координує тонкощі управління військовим нерухомим майном, зокрема елементи інтерфейсу надають змогу редагувати форми звітності та подальшого налаштування для відповідності військовим стандартам всебічної звітності та максимального спрощення контролю військових об’єктів. Усі процеси управляються за допомогою єдиної системи з управлінням персоналом, підрядниками та субпідрядниками, обслуговуванням баз та активів, складання списків, ретроспективних та статутних інструментів звітності та прогнозування, які за допомогою системи стають легко керованими [4].

На рисунку 2 зображено інтерактивну панель відображення процесів будівництва об’єктів нерухомого майна МО *RMS* з їх часовими рамками та кольором відображено стан робіт.

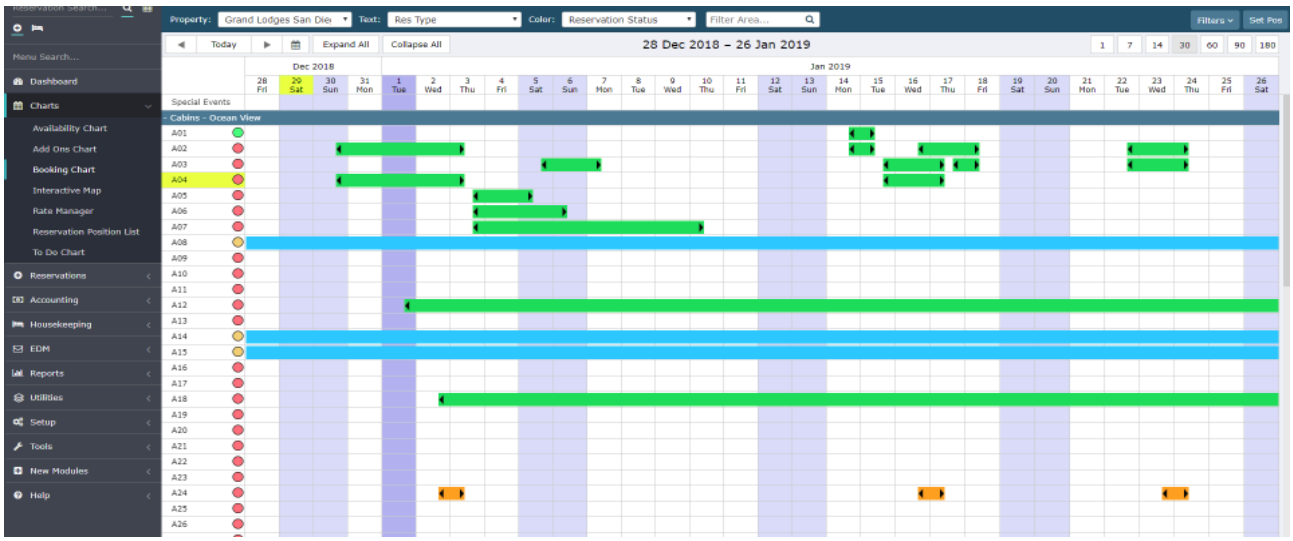

Рис. 2. Приклад списку будівельних процесів у *RMS* системі

Визначаючи важливість вище розглянутих процесів, беручи до уваги обмеження, що накладаються поточним станом в Україні, кількістю зруйнованих об’єктів, параметрами інфраструктури життєзабезпечення, робимо висновок у необхідності вибору такого варіанту архітектурної будови інформаційно-аналітичної системи МОУ, що надавала в умовах її експлуатації за призначенням найкращі показники ефективності і якості в системі підтримки прийняття рішень.

Науковий підхід розглядає прийняття рішення як єдиний комплексний процес, зміст якого дає змогу вивчити проблему, що виникла, проаналізувати можливі варіанти її вирішення і вибрати найефективніший із них. Науковий підхід забезпечує прийняття раціональних і оптимальних рішень. Раціональні рішення передбачають вибір такої альтернативи, що принесе максимум вигоди. У рамках цього підходу виникає необхідність всебічного вивчення проблеми, пошуку альтернатив і ретельного аналізу інформації. Раціональні рішення, таким чином, відрізняються від інтуїтивних тим, що базуються на об’єктивному аналітичному процесі та формально-логічному мисленні. Оптимальним рішенням називається таке, при якому досягається найкращий середній виграш. Або таке, яке приносить найкращий наслідок з найбільшою ймовірністю.

Щодо предметної області, яка розглядається, формальна постановка задачі вибору раціонального варіанту архітектури інформаційно-аналітичної системи обліку збитку та контролю відновлення зруйнованого нерухомого майна МОУ виглядає наступним чином.

Нехай є множина m варіантів архітектурної будови інформаційно-аналітичної системи підтримки прийняття рішень. Деяка j-а властивість i-го варіанта архітектурної будови характеризується величиною i-го часткового показника q_{ij}; $i=\overline{1,m}$; $j=\overline{1,n}$. Тоді архітектурна будова при i-тому варіанті реалізації характеризується вектором

$$\overline{Q_i}=\left|q_{i1},..q_{ij},..q_{in}\right|. \quad (1)$$

Завдання багатокритеріальної оптимізації зводяться до того, щоб з множини m варіантів архітектурної будови інформаційно-аналітичних систем вибрати такий варіант i_0, який має найкраще значення вектора $\overline{Q_i}$, тобто

$$i_0=\arg optQ_i,\ i=\overline{1,m}. \quad (2)$$

При цьому передбачається, що поняття „найкращий вектор $\overline{Q_i}$" – попередньо сформульований математично, тобто обраний (обґрунтований) відповідний критерій переваги (відношення переваги).

Для вирішення багатокритеріального завдання вибору необхідно виразити значення часткових показників q_{ij} у зручній кількісній формі. Найбільш доцільно як кількісні, так і якісні показники привести до вигляду, коли їхні значення змінюються від нуля до одиниці, тобто $0\le q_{ij}\le 1$ для всіх $i=\overline{1,m}$; $j=\overline{1,n}$.

При цьому кількісні показники нормуються в такий спосіб:

$$\overline{q_{ij}}=\frac{q_{ij}}{\max\limits_i q_j}, \quad (3)$$

у випадку, якщо необхідно максимізувати q_{ij},

$$\overline{q_{ij}}=\frac{\min\limits_i q_j}{q_{ij}}, \quad (4)$$

якщо необхідно мінімізувати q_{ij}.

Якісні показники подаються у вигляді експертних оцінок заданого рівня якості $\mu(q_{ij})$. Очевидно, завжди $0\le\mu(q_{ij})\le 1$.

Аналіз літератури показує, що всі численні методи вирішення багатокритеріальних завдань можна звести до трьох груп показника:

1. Метод головного показника.
2. Метод результуючого показника.
3. Лексикографічні методи (методи послідовних поступок).

Метод головного показника базується на переведенні всіх показників, крім будь-якого однорідного, що називається головним, у розряд обмежень типу рівностей та нерівностей. До недоліків методу головного показника можна віднести: труднощі виділення головного показника та встановлення припустимих значень для показників, що переводяться у розряд обмежень.

Метод результуючого показника базується на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу часткових показників на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою фахівців-експертів.

Лексикографічний метод базується на впорядкованих за важливістю показниках. Суть методу полягає у виділенні безлічі альтернатив з найкращою оцінкою за найбільш важливим показником. Якщо така альтернатива єдина, то вона вважається найкращою; якщо їх декілька, то з їхньої підмножини виділяються ті, які мають кращу оцінку за другим показником тощо.

За сукупністю показників може призначатися поступка, у межах якої альтернативи вважаються еквівалентними.

Вибір методу розв'язування багатокритеріальної задачі як у класичній, так і в нечіткій постановці визначається тим, в якому вигляді представлена експертна інформація щодо переваг показників. Якщо представлено експертну інформацію про ступінь або важливість переваги показників та визначені їхні вагові коефіцієнти, то методом розв'язування багатокритеріальної задачі вважається метод результуючого показника.

За результатами методу експертного оцінювання пропонується наступна архітектура інформаційно-аналітичної системи обліку руйнувань та контролю відновлення нерухомого майна МОУ (рис. 3).

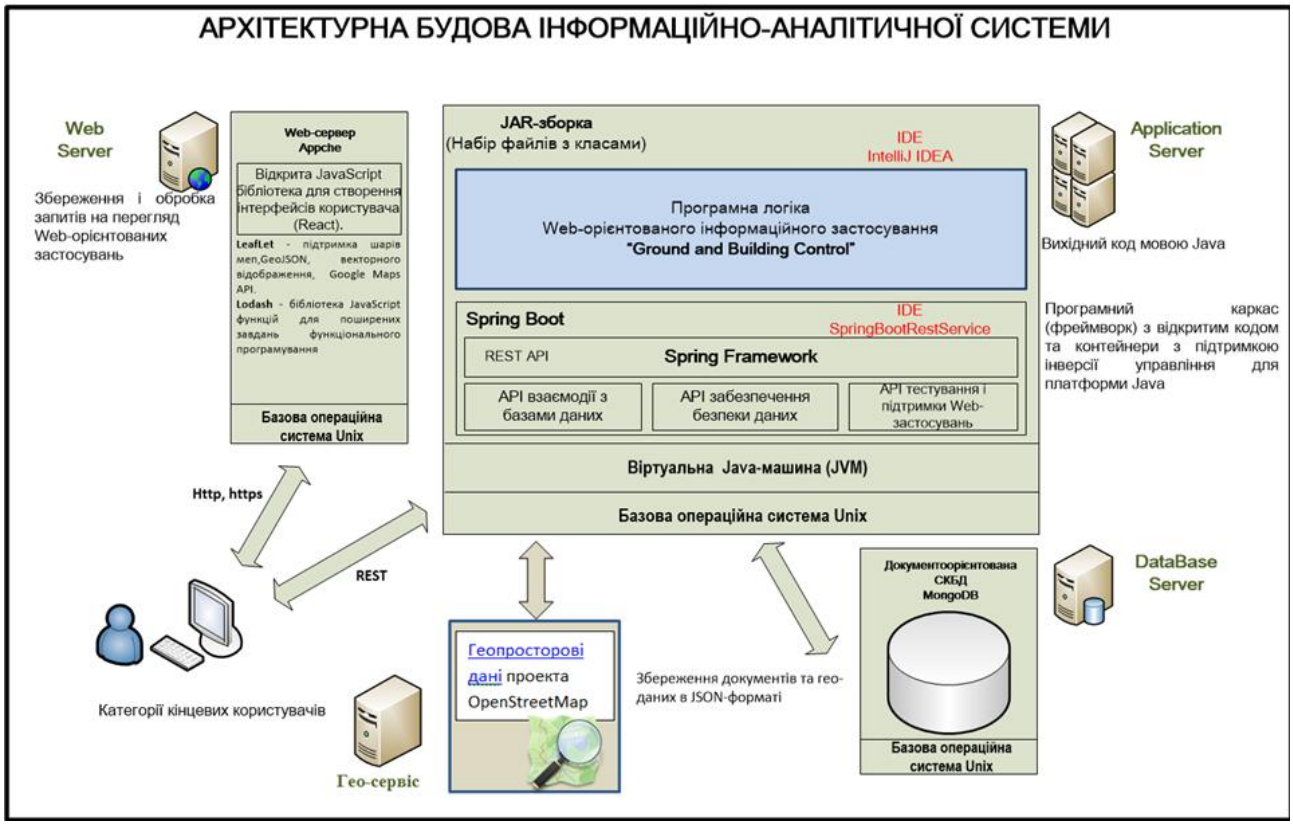

Рис. 3. Архітектурна будова прототипу геопросторової інформаційно-аналітичної системи обліку збитків та контролю відновлення зруйнованого майна МОУ

Серверний компонент повинен забезпечувати: централізовану обробку та зберігання даних, що необхідні для роботи комплексу з забезпеченням цілісності, точності та безпеки даних; формування електронних звітів інформаційно-аналітичної діяльності за визначеними критеріями; процедуру завантаження даних з різних джерел даних; базову програмну логіку підтримки прийняття рішень щодо оцінки нанесених збитків.

Клієнтський компонент призначений для забезпечення інтерактивного прикладного інтерфейсу для використання всіх функціональних потужностей системи.

Структурно прототип геопросторової інформаційно-аналітичної системи повинен складатись із наступних складових (рис. 4):

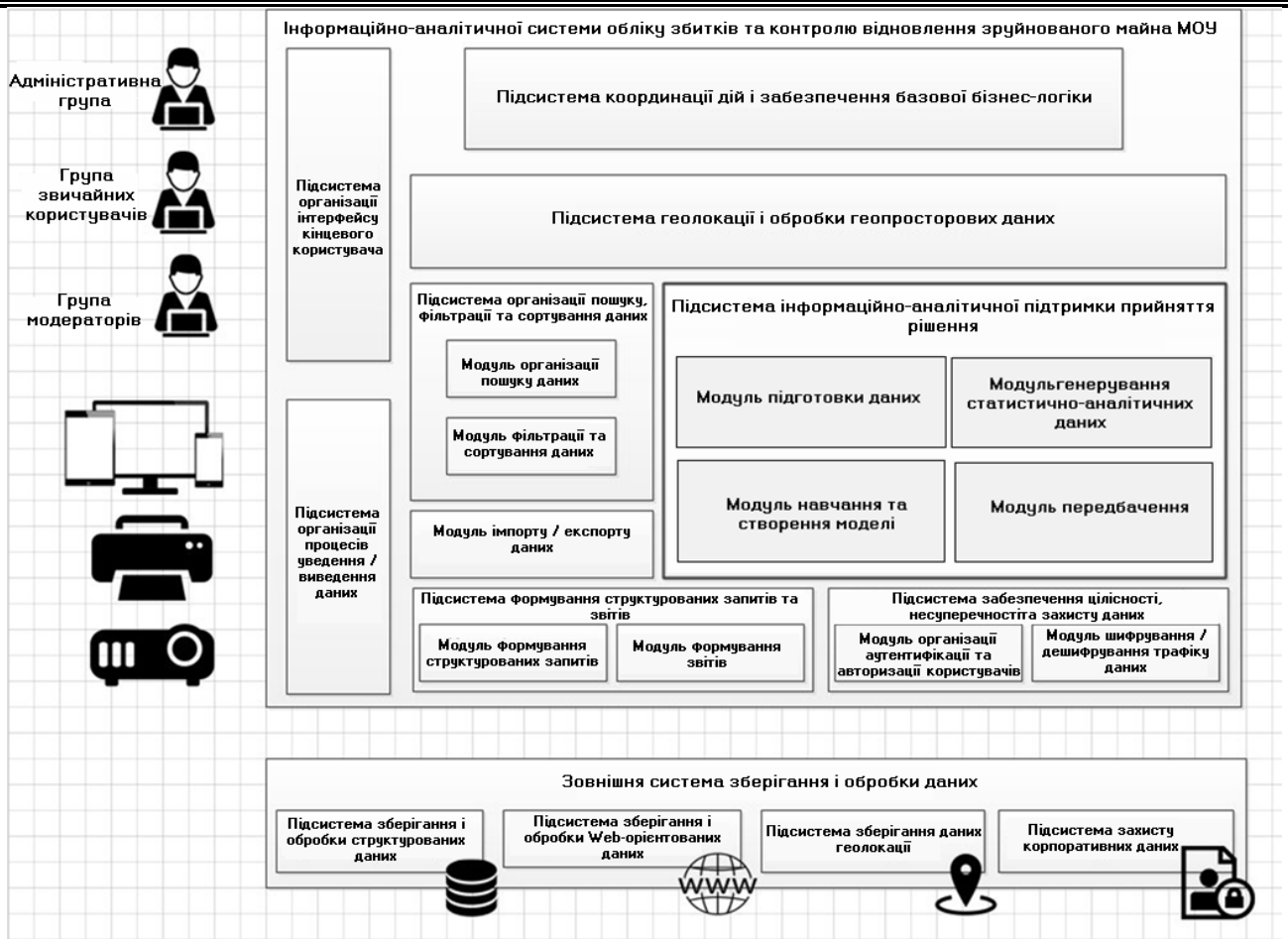

Рис. 4. Структурна схема прототипу геопросторової інформаційно-аналітичної системи обліку збитків та контролю відновлення зруйнованого майна МОУ

1. Підсистема організації інтерфейсу кінцевого користувача – забезпечує елементи інтерактивного віконного інтерфейсу для виконання базових функціональних завдань, що покладені на інформаційно-аналітичну систему.

2. Підсистема координації дій і забезпечення базової бізнес-логіки – реалізує базовий набір службових процесів, що обумовлює роботу ядра системи і координації роботи інших підсистем та модулів.

3. Підсистема геолокації і обробки геопросторових даних:

– відтворення на цифровій мапі інформації про всі об'єкти нерухомого майна, що перебувають на обліку МОУ, рівень їх руйнації або готовності для використання за призначенням після відновлювальних робіт. Дані представляються у вигляді групових і індивідуальних графічних примітивів та контекстно-залежних від них довідкових і статистичних даних;

– надання змоги виконувати маніпуляції над геоданими, іншими контекстно-залежними об'єктами предметної області автоматизації через інтерфейс адміністративної оболонки керування.

4. Підсистема організації пошуку, фільтрації та сортування даних – надає змогу здійснювати оперативний контекстно-залежний пошук даних за різноманітними критеріями, накладати фільтруючи маски для звуження або розширення інформації, що відтворюється в компонентах виводу, застосовувати різні режими сортування даних (наприклад, за алфавітом, збільшенням / зменшенням значення тощо).

5. Підсистема формування структурованих запитів та звітів – надає змогу шляхом використання спеціалізованих мов формувати інформаційні запити на виконання різнобічних операцій над даними через посередництво іменовано налаштованих джерел даних. Використовуючи генератори звітів, модуль здійснює також формування електронних звітів

статистично-аналітичної діяльності за визначеними критеріями з можливістю подальшого документування на пристроях друку, візуалізації в візуальних формах прикладного інтерфейсу, для укладання в масиви експортних структур.

6. Підсистема забезпечення цілісності, несуперечності та захисту даних. Підсистема забезпечує:

– стійку роботу системи, автоматичне відновлення у випадку виявлення системою потенційної помилки, автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу;

– несуперечливість даних та їх узгодженість з предметною областю;

– виконання операцій шифрування / дешифрування інформації, сертифікації;

– розмежування доступу до даних, запровадження прав і повноважень користувачів системи, підтримка аутентифікації та авторизації об'єктів-користувачів системи тощо.

7. Підсистема організації процесів уведення/виведення даних – забезпечує комунікативний інтерфейс взаємодії базових бізнес-процесів інформаційно-аналітичної системи з зовнішнім оточенням (програмно-апаратні засоби обчислювальної техніки, програмно-апаратні комплекси тощо).

8. Модуль імпорту/експорту даних – надає змогу виконати упаковування (розпаковування) даних в (з) формати інших джерел.

9. Модуль формування довідкової інформації про роботу із системою – надає змогу отримувати контекстно-залежну довідку про узагальнену функціональність системи, порядок взаємодії з інтерфейсом користувача і виконання головних завдань, що покладені на систему в цілому або її складові підсистеми.

Ключовим елементом інформаційно-аналітичної системи виступає **Підсистема інформаційно-аналітичної підтримки прийняття рішення.**

На неї покладаються наступні завдання (рис. 5):

– отримання статистично-аналітичних даних по всіх об'єктах МОУ, що підляглися руйнації, пошкодженню в результаті ведення бойових дій;

– отримання прогнозу на стан робіт по відновленню об'єкта (ремонт/реконструкція).

Слід відзначити, що дана підсистема є головним елементом системи прийняття рішень і спрямована на отримання знань про об'єкт дослідження – виявлення корисної інформації, отримання висновків, врешті, підтримка в прийнятті розумного (зваженого) рішення. Дане рішення має бути основане не на поверхневих знаннях про об'єкт, а на аналізі багатьох факторів, які можуть непрямо відноситися до об'єктів, які дозволяють користувачам отримувати інформацію або знання з інформаційної системи.

Одержання вірних рішень по сучасних системах є наукомістким, тому є необхідними обробка та управління знаннями. Так само, як комп'ютерні науки продукують технологічну основу для реалізації систем підтримки прийняття рішень, управління знаннями утворює інтелектуальну базу для розробки, вивчення і застосування систем підтримки прийняття рішень [5].

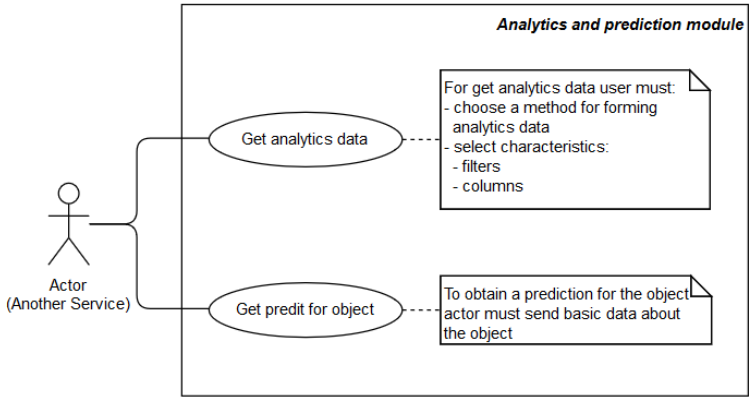

Рис. 5. Діаграма варіантів використання *(use case diagram)*

Під час фази дослідження (рис. 6) керівник військового управління або система управління отримує дані, які опрацьовуються, і синтезується інформація (нові відомості про об'єкт дослідження, що ми отримали з даних). Далі здобута інформація на фазі проєктування структурується, виводяться судження, які розглядаються, аналізуються, і наприкінці приймається управлінське рішення [5].

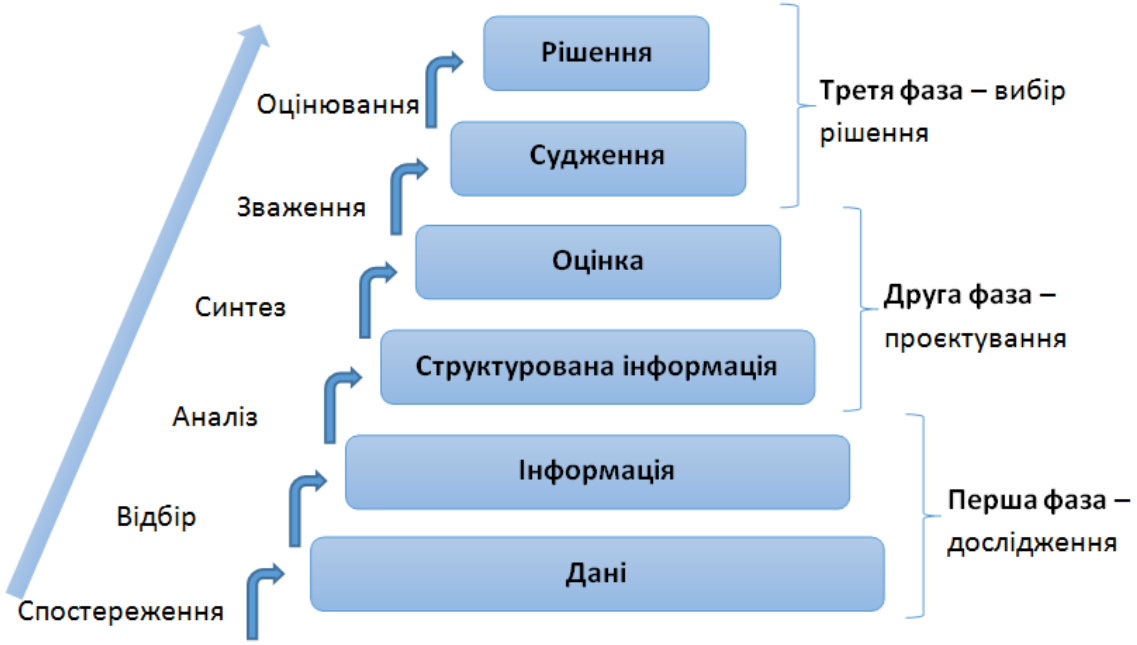

Рис. 6. Формалізація алгоритму прийняття рішення

Динаміка трансформації інформації в контурі підтримки прийняття рішень інформаційно-аналітичної системи обліку збитків та контролю відновлення зруйнованого майна МОУ представлена в таблиці 1.

Таблиця 1

Ілюстрація фаз одержання знань

Фази отримання знань	**Результат**
Дані	26
Інформація	26 % – будівельна готовність за результатами руйнації
Структурована інформація	26 % – будівельна готовність казарми № 1 смт Петровичі станом на 13–14.10.2022 з кількістю будівельників 4
Судження	Відновлення казарми № 1 буде завершено не вчасно за даних умов
Рішення	Збільшити кількість робітників на об'єкті казарма № 1 смт Петровичі до 14 осіб

Аналіз існуючих підходів в реалізації спеціалізованих СППР обумовив віддати перевагу в сторону гібридних, що в більшості представлені в предметній області, що розглядається.

Існує два основні підходи до інтеграції СППР: вкладеність і синергія. Методи вкладення припускають передачу властивостей інвестиційної системи системі, яка отримала цю підсистему.

У синергетичному підході до інтеграції різних систем немає вкладеності, немає домінуючої технології, немає вкладених систем і методів. Всі методи інтегровані в один інструмент, що дозволяє використовувати їх незалежно один від одного або разом кількома методами в рамках однієї операції [6].

Такий варіант структури СППР найкраще підходить для вирішення задач, поставлених перед інформаційно-аналітичною системою обліку збитків та контролю відновлення зруйнованого майна МОУ. Завдяки такій структурі СППР можна побудувати модель, котра базується на методах штучного інтелекту, а також додати систему формування інтерактивних

звітів, які будуть узагальнено та лаконічно представляти інформацію на основі графічної візуалізації (рис. 7).

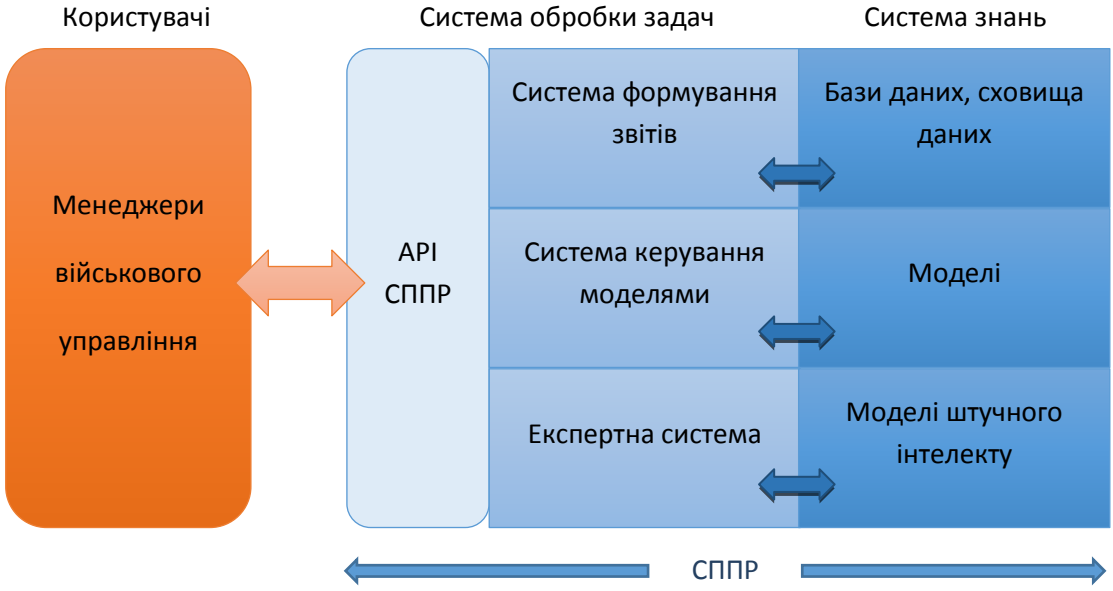

Рис. 7. Варіант гібридної структури СППР

Системи підтримки прийняття рішень використовують математичні моделі для отримання науково-обґрунтованих адміністративних рішень. Найпопулярнішими з них є такі типи моделей: оптимізація, статистичний аналіз, прогнозування, нейронні мережі [7]. Модель оптимізації описується критерієм оптимізації (цільовою функцією) та обмеженнями.

Огляд математичної моделі можна представити наступним чином.

$$p = \min f_0(x), \tag{5}$$

обмеження $f_i(x)\ b_i\ i = 1, \dots, m.$

За предметною областю дослідження цільова функція повинна бути спрямована на мінімізацію:

– кількості будівельних засобів та матеріалів, що вимагаються для відновлення зруйнованих та пошкоджених об'єктів МОУ;

– чисельності колективу інженерно-будівельних спеціалістів, що задіються для виконання завдань відновлення об'єктів відповідно до встановлених смет;

– вартості виконання завдання для приведення об'єкту МОУ до застосування за призначенням;

– термінів часу на заплановані етапи відбудови.

Обмеженнями предметної області виступають: кошторис на будівництво (відбудову, ремонт); терміни часу перебування об'єкту МОУ в зоні окупації; інші ситуаційні фактори.

Аналіз досвіду світової практики у вирішенні подібного роду завдань, переліку завдань, що висуваються перед підсистемами інформаційно-аналітичної підтримки прийняття рішення, обумовив взяти за основу модель на основі нейронної мережі, тобто, модель, що використовує штучну мережу і підтримує нечітку логіку. Також ця модель підходить для вирішення задачі по прогнозуванню вірогідності вчасного завершення робіт, так як дані, надані замовником, є в більшості неструктурованими та мають багато пропусків (не заповненні поля та значення, які підпадають в категорію аномалій).

Архітектура підсистеми інформаційно-аналітичної підтримки представлена на рисунку 8.

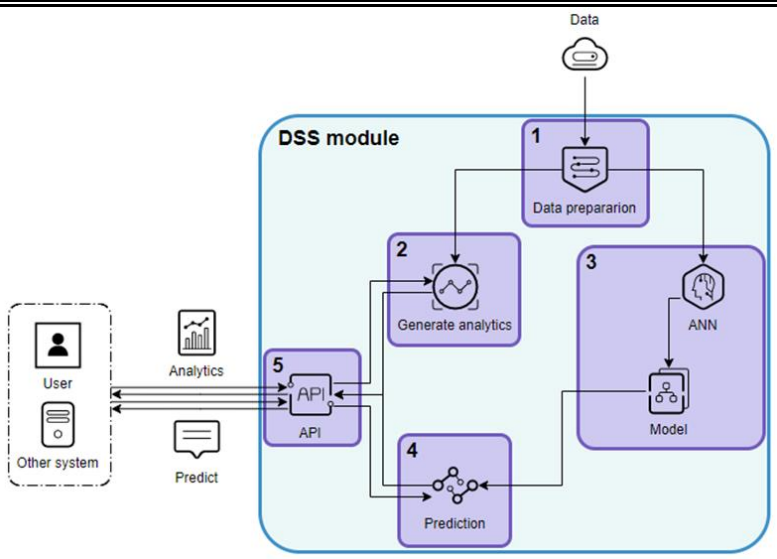

Рис. 8. Архітектура підсистеми інформаційно-аналітичної підтримки прийняття рішення:
1 – Модуль підготовки даних; 2 – Модуль генерування САД; 3 – Модуль навчання та створення моделі;
4 – Модуль передбачення; 5 – *API* для взаємодії з користувачем (сервісом)

Діаграма послідовностей реалізації завдань, що покладаються на підсистему інформаційно-аналітичної підтримки прийняття рішення, описує процеси взаємодії користувача і сервісу (рис. 9) [8].

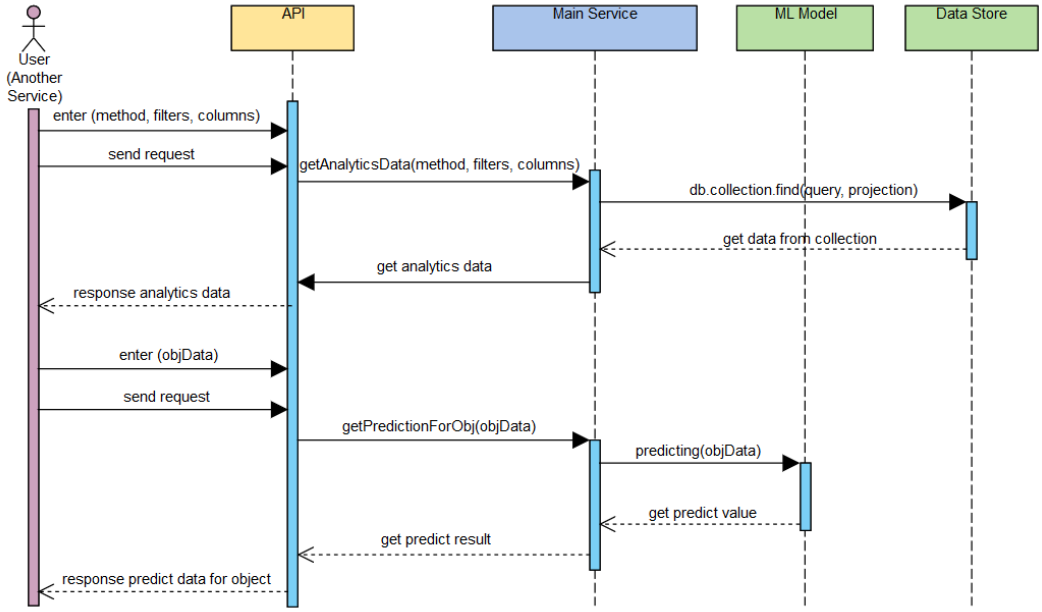

Рис. 9. Діаграма послідовностей (*sequence diagram*)

В запиті на отримання статистично-аналітичних даних користувач вибирає метод формування даних та характеристики. Далі відправляється запит на отримання даних з вказаними характеристиками до сховища даних. Отримані дані зі сховища трансформуються в статистично-аналітичні дані за заданим методом. Для отримання передбачень від користувача (сервісу) на сервіс відправляється запит з об'єктом, на який потрібно зробити передбачення на вірогідність завершення виконання робіт вчасно, сервіс повертає значення передбачення в межах [0, 1].

Послідовності бізнес-процесів або дій, реалізованих методами класів (процедурами), по побудові *ML*-моделі для підсистеми підтримки прийняття рішень можна представити наступним чином:

1. Підготовка статистичних даних:

– визначення переліку атрибутів даних, що підлягають обробці за предметною областю дослідження;

– видалення дублюючої інформації для максимального зменшення показника збитковості;

– приведення типів даних до встановлених в інформаційно-аналітичній системі еталонних стандартів;

– заповнення пропущених даних, що за певних обставин не визначені на етапі постачання і валідації інформації;

– нормалізація числових даних. Це потрібно для адекватного застосування математичних методів і комп'ютерних розрахунків при пов'язаних із великими і малими абсолютними величинами обчисленнях, а також для того, аби встановити відповідність між кількісними та якісними значеннями;

– очищення від аномалій;

– спрощення даних.

2. Створення моделі:

– вибір методу;

– підбір глобальних параметрів;

– тренування моделі;

– оцінка моделі.

Крім цього є проміжні та фінальні дії: збір даних, поділ даних на тренувальні та для тестів, вибір моделі з найкращою точністю.

Результатом роботи модуля є сформований набір статистично-аналітичних даних, який можна отримати з *API* підсистеми. Нижче наведено приклад візуалізації статистично-аналітичних даних, які надав модуль (рис. 9).

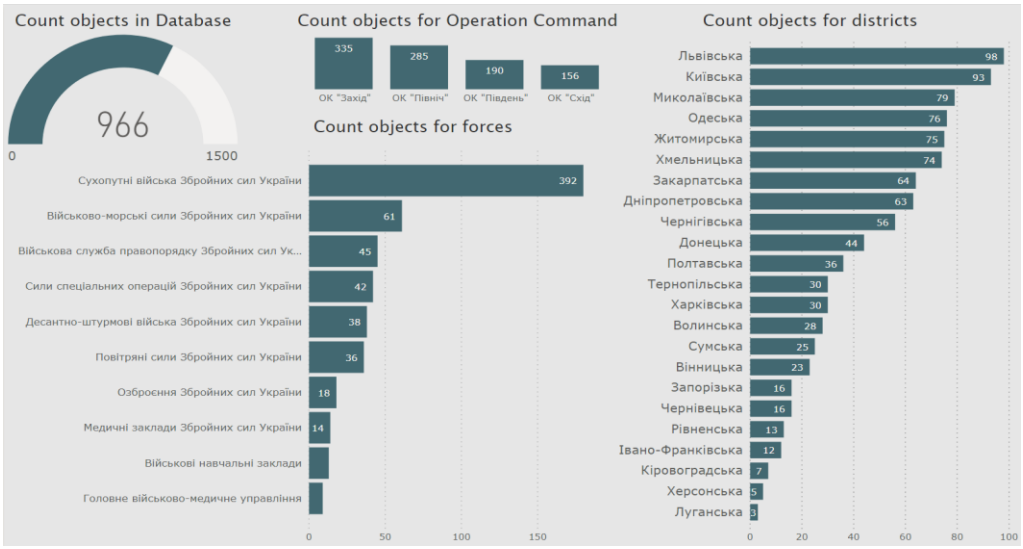

Рис. 9. Візуалізація даних, наданих модулем формування статистично-аналітичних даних

Висновок. Досвід впровадження засобів електронного обліку будівництва об'єктів Міністерства оборони країн-членів НАТО обумовлює преломлення процесів діджиталізації у даній предметній області в бік усунення наслідків військової агресії російської федерації.

Науковий підхід розглядає прийняття рішення як єдиний комплексний процес, зміст якого дає змогу вивчити проблему, що виникла, проаналізувати можливі варіанти її вирішення і вибрати найефективніший із них.

Вибір раціональної архітектури інформаційно-аналітичної системи зводиться до обґрунтованого вибору методу розв'язання багатокритеріальної задачі, як у класичній, так і в нечіткій постановці.

Ключовим елементом структурної будови інформаційно-аналітичної системи виступає підсистема інформаційно-аналітичної підтримки, що відповідає гібридній моделі реалізації СППР. Дана модель використовує штучну нейронну мережу і підтримує нечітку логіку. Це

надає можливості для вирішення задачі з прогнозування вірогідності вчасного завершення відновлювальних робіт об'єктів руйнації.

Результати виконання бізнес-процесів гібридної СППР доводять доцільність застосування методів *Machine Learning* у ефективності прийняття якісного рішення.

В подальших дослідженнях планується оцінити ефективність запропонованого підходу за методом *Machine Learning* порівняно з існуючими підходами.

ЛІТЕРАТУРА

1. Про затвердження Змін до Інструкції з обліку військового майна у Збройних Силах України: Наказ Міністра оборони України від 10.07.2019 № 373 // Офіційний вісник України. 2019. № 64. С. 142.

2. Про затвердження Інструкції з обліку військового майна у Збройних Силах України: Наказ Міністра оборони України від 17.08.2017 № 440 // Офіційний вісник України. 2017. № 86. С. 93.

3. MilCon Dashboard Capability Requirements Document - Office of the Assistant Secretary of Defense (Energy, Installations, & Environment) Business Systems & Information Directorate. January, 2016.

4. Quality Control System (QCS) and Resident Management System (RMS). URL: https://www.swf.usace.army.mil/Portals/47/docs/CQM/Guide/Module_8.pdf.

5. Лінькова О. Ю. Основи управлінського консультування: навч.-метод. посіб. / Лінькова О. Ю., Соколенко В. А. 3-тє вид. Харків: МарТ, 2018. 526 с.

6. Орлов А. І. Прийняття рішень. Теорія і методи розробки управлінських рішень: навч. посіб. 3-те вид. Харків: МарТ, 2015. 415 с.

7. Демиденко М. А. Системи підтримки прийняття рішень для прийняття управлінських рішень: навч. посіб. Нац. гірн. ун-т, 2017.

8. *UML* діаграма послідовності. URL: https://studfile.net/preview/5200239/page:6/#13.

УДК 621.391
Ольшанський В. В. ORCID: 0000-0002-5788-8173 (ВІТІ)
Філіпов В. В ORCID: 0000-0001-7854-6693 (ВІТІ)

АНАЛІЗ СИСТЕМ РАДІОЗВ’ЯЗКУ ЗА ПОКАЗНИКАМИ ЕФЕКТИВНОСТІ

У статті 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 більш повною й більш конкретною та 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 виконана 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.

Ключові слова: *енергетична ефективність, сигнально-кодові конструкції, кодек.*

V. Olshanskiy, V.Filipov Analysis of radio communication systems by performance indicators.

The article deals with the analysis of radio communication systems based on performance indicators. It was established that modern complex radio communication systems cannot always be comprehensively characterized by one indicator. Evaluation by several indicators is more complete and more specific and allows to characterize various properties of the system. Optimization of the transmission system as a whole, i.e. taking into account encoding and decoding devices, is carried out on the basis of information theory.

The most general evaluation of the efficiency of the communication system is the ratio of channel utilization by bandwidth (information efficiency). To ensure a given speed of information transmission and a given probability, it is necessary to spend some signal power and occupy a certain frequency band in the communication channel. What power and what frequency band will be needed depends on the communication system used.

The efficiency of the information transmission system is evaluated by the coefficient of signal power utilization (energy efficiency) and the coefficient of channel bandwidth utilization (frequency efficiency). An increase in frequency efficiency requires an increase in energy costs (a decrease in energy efficiency).

With high requirements for fidelity of transmission, it becomes expedient to use interference-resistant codes, which allow to increase energy efficiency in exchange for reducing the specific speed of information transmission. The simultaneous requirement of high speed and fidelity of information transmission in conditions of limited frequency and energy resources can be fulfilled by the joint use of multi-position signals and powerful interference-resistant codes.

To assess the energy efficiency of radio communication systems, it is advisable to use the signal power utilization factor. The advantages of increasing energy efficiency are obvious: minimization of transmitter radiation power, improvement of electromagnetic compatibility of radio-electronic devices, increase of stealth of information transmission, minimization of energy consumption.

Keywords: *energy efficiency, signal-code constructions, codec.*

Постановка завдання

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 [1], 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 теорії завадостійкості оптимізація приймальної частини цифрової системи передачі інформації здійснюється на основі критерію мінімуму ймовірності помилки (критерію ідеального спостерігача) [2]. Однак, на підставі методів теорії завадостійкості вдається оптимізувати достатньо повно лише алгоритми обробки сигналу при прийманні. Вирішити ж завдання вибору оптимального закону модуляції, і особливо оптимального кодування, на базі цієї теорії не вдається. Критерій мінімуму ймовірності помилки є досить повним для систем без кодування. У цих системах оптимізація фактично зводиться до оптимізації модему. У системах з кодуванням завдання істотно ускладнюється. Тут у формуванні і обробці сигналу важлива роль приділяється кодекам. Основним показником якості таких систем стає швидкість передачі, при якій забезпечується задана ймовірність помилки.

Аналіз публікацій за темою дослідження

Відомо, що сучасні принципи організації зв'язку і технічні характеристики засобів радіозв'язку підрозділів зв'язку Збройних сил України не дозволяють цілком задовольнити потреби управління військами в умовах сучасного бою. Системи радіозв'язку складаються з великої номенклатури обладнання (антеннофідерні пристрої, маршрутизатори, шлюзи, комутатори, сервери і т. ін.). Особливістю обладнання сучасних систем радіозв'язку є цифровий спосіб оброблення інформації та комутації.

Кількісною мірою якості системи радіозв'язку, як складної системи, є критерій ефективності. Критерій ефективності повинен відповідати функціональному призначенню системи, мати чіткий фізичний зміст, давати однозначну кількісну оцінку, бути простим, ураховувати основні параметри системи. Складна система може бути описана сукупністю показників якості, кожен з них характеризує одну з властивостей системи. Узагальнений критерій ефективності, що враховує всю сукупність показників якості, є складним, і формальні методи синтезу систем за таким критерієм ще недостатньо розроблені. Тому на практиці порівняння систем роблять за одним найбільш істотним приватним критерієм ефективності, а на інші накладаються обмеження. Застосування сукупності приватних критеріїв ефективності дозволяє аналізувати різні сторони роботи системи і формулювати конкретні вимоги до її елементів, що важливо для практики.

У той же час передача інформації в різних системах з однаковою якістю ще не дає підстави для судження про те, гарні вони чи погані. Для системи зв'язку, як для будь-якої складної системи, варто враховувати ряд інших її показників, що характеризують: потужність сигналу, займану смугу частот, відношення сигнал/шум і т. ін. Система зв'язку повинна забезпечувати передачу інформації з максимальною правильністю при обмеженнях на потужність, смугу частот, вартість устаткування. Засоби зв'язку, які дозволять одержати більш високі показники правильності передачі інформації при однакових витратах, будуть більш ефективними [11].

Тому, сучасні складні системи зв'язку не завжди можуть бути вичерпно охарактеризовані одним показником. Оцінка за декількома показниками є більш повною і більш конкретною та дозволяє охарактеризувати різні властивості системи. Оптимізація системи передачі в цілому, тобто з урахуванням пристроїв кодування й декодування, здійснюється на основі теорії інформації, основи якої розроблені К. Шенноном [3; 7].

Метою статті є аналіз систем радіозв'язку за показниками ефективності.

Виклад основного матеріалу

Під ефективністю системи зв'язку розуміється її здатність забезпечити передачу інформації найбільш достовірним способом.

При виборі комплексного показника ефективності системи виходять із того, що він повинен мати прямий зв'язок з її цільовим призначенням, об'єктивно характеризувати основні властивості, бути чутливим до зміни визначальних параметрів системи та поряд з цим повинен бути досить простим, щоб їм можна було скористатися. Проблема полягає в тому, що не всі цілі системи можна адекватно відобразити у кількісній формі. Тим не менш, вирішення питань вибору найбільш доцільних варіантів системи зв'язку зрештою зводиться до вирішення завдань оптимізації цих систем за вибраними критеріями якості.

Найбільш загальною оцінкою ефективності системи зв'язку є коефіцієнт використання каналу за пропускною здатністю (інформаційна ефективність), який дорівнює відношенню швидкості передачі інформації до пропускної здатності:

$$\eta = \frac{v_{\text{і}}}{C}. \tag{1}$$

Інформаційна ефективність η завжди менше одиниці, що ближче η до одиниці, то досконаліша система.

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. Зацікавлює порівняти між собою різні системи зв'язку за ступенем ефективності використання ними основних ресурсів каналу: пропускної здатності, потужності сигналу і займаної смуги частот.

Ефективність системи передачі інформації оцінюється коефіцієнтом використання потужності сигналу β_E (енергетичною ефективністю)

$$\beta_E = \frac{v_{\text{і}}}{P_{\text{с}}/G_0} \tag{2}$$

і коефіцієнтом використання смуги частот каналу β_F (частотною ефективністю) [6; 8]

$$\beta_F = \frac{v_{\text{і}}}{\Delta F}, \tag{3}$$

де G_0 – спектральна щільність потужності шуму;

$P_{\text{с}}$ – потужність сигналу;

ΔF – смуга пропускання каналу зв'язку.

Граничні можливості системи передачі інформації можна оцінити за допомогою виразу для пропускної здатності Гаусівського безперервного каналу зв'язку зі смугою частот ΔF, з урахуванням формули Шеннона:

$$C = \Delta F \log_2\left(1 + \frac{P_c}{P_з}\right) = \Delta F \log_2(\rho + 1), \tag{4}$$

де $\rho = P_c/P_з$ відношення потужності сигнал та завада в смузі ΔF отримуємо наступні вирази:

$$\eta = \frac{\beta_F}{\log\left(\frac{\beta_F}{\beta_E + 1}\right)}, \qquad \beta_F = \rho\beta_E. \tag{5}$$

При відповідних способах передачі і прийому величина η може бути скільки завгодно близька до одиниці, при цьому помилка може бути скільки завгодно малою. У цьому випадку маємо граничну залежність між β_E та β_F у вигляді:

$$\beta_E = \frac{\beta_F}{2^{\beta_F} - 1} \tag{6}$$

Наочно ця залежність представляється у вигляді кривої на β_E та β_F площині (рис. 1), вона відбиває найкращий обмін між β_E та β_F у безперервному каналі.

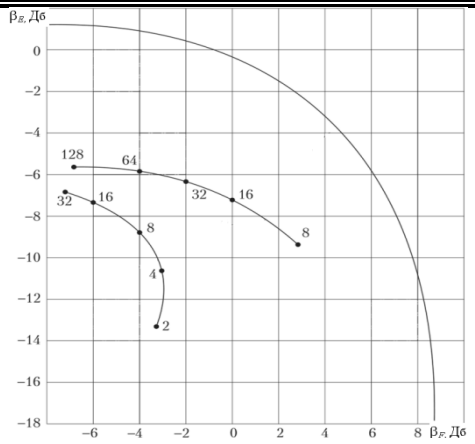

Рис. 1. Криві енергетичної та частотної ефективності

З аналізу співвідношення (6) та межі Шеннона показує, що підвищення частотної ефективності (тобто зниження витрат смуги $1/\beta_F$) вимагає збільшення енергетичних витрат (зниження енергетичної ефективності).

Частотна ефективність β_F змінюється в межах від 0 до 2 біт·с$^{-1}$/Гц для двійкових сигналів (межа Найквіста), до $2\log_2 M$ біт·с$^{-1}$/Гц для M-позиційних сигналів (де M – обсяг сигнального ансамблю). Енергетична ефективність обмежена зверху величиною

$$\beta_{F\max} = \frac{\lim}{\beta_F}\beta_E = \frac{\lim}{\beta_F}\frac{\beta_F}{2^{\beta_F}-1} = \frac{1}{\ln 2} \tag{7}$$

Застосування методів багатопозиційної маніпуляції підвищує питому швидкість передачі β_F. При цьому збільшення M призводить до зменшення відстані між найближчими сигнальними точками ансамблю ($d_{\min}$) [10], що веде до 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 виконана при спільному використанні багатопозиційних сигналів і потужних завадостійких кодів.

Створення систем передачі, у яких досягаються близькі до граничного показники ефективності, вимагає спільного узгодження кодека і модему з урахуванням статистичних властивостей безперервного каналу. Це означає, що кодування і модуляцію необхідно розглядати як єдиний процес формування сигналу, а демодуляцію і декодування – як процес оптимального в цілому прийому сигнально-кодового блоку. Спільна оптимізація модемів і кодеків дозволяє істотно знизити втрати інформації, а комбінування різних ансамблів сигналів і завадостійких кодів породжує безліч варіантів побудови таких систем.

Комбінування різних ансамблів M-позиційних сигналів, завадостійких і маніпуляційних кодів породжує безліч конструкцій. Однак тільки узгоджені варіанти цих конструкцій забезпечують підвищення частотно-енергетичної ефективності систем передачі інформації. Такі варіанти називають сигнально-кодовими конструкціями (СКК) [7; 9].

Введення поняття СКК відображує підхід до модуляції і кодування як процесу об’єднання сигналів і кодів у єдину енергетично- і частотно-ефективну конструкцію та пов’язані з цим специфічні проблеми, які не розглядають у звичайних варіантах "кодек-модем". Ідея побудови СКК полягає в збільшенні мінімальної евклідової відстані між дозволеними кодованими сигнальними послідовностями з використанням надлишковості кодування. При цьому асимптотичний енергетичний виграш кодування (ЕВК) визначається формулою:

$$\beta_{\text{кк}} = 20\lg\frac{d_E}{d_{E\min}}, \tag{8}$$

де

$$d_E = \|\mathbf{x}-\mathbf{y}\| = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad - \tag{9}$$

вільна евклідова відстань між дозволеними кодовими блоками x_i і y_i;

$d_{E\,\min}$ − мінімальна евклідова відстань між різними послідовностями в системі без кодування з однаковою середньою або піковою потужністю.

Для одержання більших величин ЕВК при побудові СКК необхідно підбирати коди, які максимізують вільну евклідову відстань.

Застосування завадостійкого кодування не повинне викликати розширення смуги частот або зменшення швидкості передачі повідомлень. Збільшення кількості позицій використовуваних сигналів дозволяє вирішити цю проблему.

Для військових систем радіозв'язку, де, як правило, інформаційне навантаження на напрямках зв'язку є відомим, більш актуальною є задача підвищення енергетичної ефективності при обмеженнях на пропускну спроможність, смугу пропускання та достовірність. Для оцінки енергетичної ефективності систем і засобів радіозв'язку доцільно застосовувати коефіцієнт використання потужності сигналу β_E. Переваги підвищення енергетичної ефективності очевидні: мінімізація потужності випромінювання передавача, покращення електромагнітної сумісності радіоелектронних засобів, підвищення прихованості передачі інформації, мінімізація енергоспоживання.

Висновки

У статті проведений аналіз систем радіозв'язку за показниками ефективності, який показує, що сучасні складні системи радіозв'язку не завжди можуть бути вичерпно охарактеризовані одним показником. Оцінка за декількома показниками є більш повною й більш конкретною та дозволяє охарактеризувати різні властивості системи.

Для оцінки ефективності систем радіозв'язку доцільно застосувати коефіцієнт використання потужності сигналу β_E. Величина β_E залежить від виду сигналу, виду та інтенсивності завади.

Напрямком подальших досліджень є розробка математичної моделі спотворення сигналу при впливі навмисних завад.

ЛІТЕРАТУРА

1.Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Москва: Вильямс, 2003. 1104 с.

2. Кувшинов О. В., Лівенцев С. П., Лежнюк О. П., Міночкін А. І., Могилевич Д. І. Теорія електричного зв'язку: підруч. Київ: ВІТІ НТУУ „КПІ", 2008. Ч. 2: Основи теорії завадостійкості, кодування та інформації. 286 с.

3. Борисов В. И. и др. Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. Москва: Радио и связь, 2000. 384 с.

4. Шишацький А. В. Розвиток інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил / А. В. Шишацький, О. М. Башкиров, О. М. Костина // Озброєння та військова техніка. Київ: ЦНДІ ОВТ ЗС України, 2015. № 1 (5). С. 35–40.

5. Толюпа С. В. Аналіз методів оцінки багатопроменевого каналу зв'язку / С. В. Толюпа, Т. Г. Гурський, О. І. Восколович // Збірник наукових праць „Вісник ДУІКТ". 2011. Вип. 2. С. 21–27.

6. Воронин А. М. Многокритериальный синтез динамических систем. Київ: Наукова думка, 1992. 160 с.

7. Брахман Т. Р. Многокритериальность и выбор альтернатив в технике. Москва: Радио и связь, 1984. 288 с.

8. Герасимов Б. М. Человекомашинные системы принятия решений с элементами искусственного интеллекта / Б. М. Герасимов, В. А. Тарасов, И. В. Токарев. Київ: Наукова думка, 1993. 181 с.

9. Берштейн Л. С. Нечеткие модели принятия решений: дедукция, индукция, аналогия: монография / Л. С. Берштейн, А. В. Боженюк. Таганрог: Изд-во ТРТУ, 2001. 110 с.

10. Борисов А. Н. Обработка нечеткой информации в системах принятия решений / А. Н. Борисов, А. В. Алексеев, Г. В. Меркурьева. Москва: Радио и связь, 1989. 304 с.

11. Бондаренко І. М. Системи радіозв'язку: навч. посіб. Харків: ХІ ВПС, 2003. Кн. 2, ч. 1: Радіолінії зв'язку. 162 с.

УДК: 400:002.1

Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ)
Слотвінська Л. І. ORCID: 0000-0003-2409-6206 (ВІТІ)
Ляшенко В. О. (А0515)

ВАРІАНТ СИСТЕМИ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ НА ОСНОВІ 2D (QR) КОДУ

Завдяки розвитку цифрових технологій у сучасному світі значно підвищились вимоги до систем життєзабезпечення та діяльності суспільства, а також до документів, що беруть участь у роботі цих систем.

Прикладів таких систем безліч і майже всі вони використовують документи у вигляді пластикової картки. Оскільки це документи, то актуальними є питання захищеності систем від несанкціонованого доступу, а саме, наявність елементів захисту та надійність процесів ідентифікації та автентифікації користувачів.

В статті проаналізовано існуючі «електронні елементи захисту» й електронні елементи персоналізації сучасних документів, а саме види, характеристики, процеси функціонування.

Проведено оцінку електронних елементів захисту.

Встановлено, що на ступінь захищеності документу впливають два основні чинники, такі як контроль доступу та проведення процедури зчитування, захищеної базовим контролем доступу.

Запропоновано систему захисту на основі елементу персоналізації.

Така система може бути використана як аналог більш дорогим варіантам організації контрольно-пропускного режиму на об'єктах, завдяки своїй простоті, малоймовірності несанкціонованого доступу до алгоритмів та процесу роботи її елементів. Впровадження даної системи на контрольно-пропускних пунктах може значно покращити управління та забезпечити захищеність системи безпеки, процесу перетину контрольованої зони.

Напрямком подальших досліджень є розробка системи з переносом персоналізованої інформації з документів напряму до баз даних машинозчитуваних систем.

Однак найважливішим параметром залишиться стійкість та захищеність від несанкціонованого втручання в роботу машинозчитуваних електронних систем.

Ключові слова: *система контролю й управління доступом, машинозчитуваний проїзний документ, технологія радіочастотної ідентифікації, двовимірний штрих-код, базовий контроль доступу, автентифікація чіпа.*

I. Panchenko, L. Slotvinskaya, V. Lyashenko. Variant of electronic identification and authentification system based on 2D (QR) code.

Due to the development of digital technologies in the modern world, the requirements for life support systems and society, as well as for the documents involved in the work of these systems have increased significantly.

There are many examples of such systems and almost all of them use documents in the form of a plastic card. As these are documents, the issues of protection of systems from unauthorized access are relevant, namely, the availability of security features and the reliability of the processes of identification and authentication of users.

The article analyzes the existing "electronic elements of protection" and electronic elements of personalization of modern documents, namely the types, characteristics, processes of functioning.

The evaluation of electronic security elements was carried out.

It is established that the degree of security of the document is influenced by two main factors, such as access control and reading procedure, protected by basic access control.

A protection system based on the personalization element is proposed.

Such a system can be used as an analogue of more expensive options for the organization of access control at facilities, due to its simplicity, the likelihood of unauthorized access to algorithms and the process of its elements. The implementation of this system at checkpoints can significantly improve the management and security of the security system, the crossing process controlled area.

The direction of further research is the development of a system with the transfer of personalized information from documents directly to the databases of machine reading systems.

However, the most important parameter will remain the stability and protection against unauthorized interference in the operation of machine-readable electronic systems.

Keywords: *access control and management system, machine-readable travel document, radio frequency identification technology, two-dimensional bar code, basic access control, chip authentication.*

Постановка завдання та актуальність дослідження

Як в умовах функціонування силових структур, так і в умовах ведення гібридної війни між Україною і Росією, в тому числі на сході України та в зоні проведення Операції об'єднаних сил, дуже часто виникає потреба в мобільному та швидкому створенні пропускних пунктів, де проводиться контроль великого потоку людей з використанням різного виду документів.

Значну частину складають документи, що контролюються в автоматичному або напівавтоматичному режимах [1–7; 9].

Такі документи оснащені машинозчитуваними елементами і дістали назву машинозчитувані проїзні документи (МЗПД). Їх перевірка відбувається з використанням електронної бази даних.

Загальні вимоги до виготовлення і функціонування МЗПД викладені в стандарті «ICAO Doc 9303 Машинозчитувані проїзні документи» [12].

Згідно з нормативними документами МЗПД повинні мати поліграфічний захист від підробок, який не повинен заважати машинному зчитуванню, а також електронний елемент захисту.

Електронний елемент захисту – це електронний носій із закодованою інформацією, яка зчитується за допомогою спеціальних електронних пристроїв і програмного забезпечення.

Різноманітні електронні елементи захисту мають свої переваги і недоліки. Але, однозначно, що використання електронної бази даних, відповідних документів з машинозчитуваними елементами та програмно-апаратного комплексу може значно полегшити процедуру контролю та забезпечити безпеку роботи органів і підрозділів, які працюють з документами.

Аналіз публікацій за темою дослідження

Для захисту документів використовують різні електронні елементи персоналізації, такі як *магнітна смуга, 1D та 2D штрих-коди, а також різновиди чипів та міток.* Дані методи полягають у захищеності електронної системи від несанкціонованого доступу до неї, сприяють запобіганню пошкодження, зміни чи викрадення інформації, яка міститься на машинозчитуваних закодованих елементах [1].

На теперішній час рівень інтеграції машинозчитуваних систем захисту й обробки персональних даних на документах перебуває на високому рівні. Створено безліч інститутів та стандартів щодо технологічних процесів виготовлення, використання та їх захисту.

Для створення ідентифікаційних та інших документів сьогодні використовують найсучасніші технології. Однак існують факти їх підробки, несанкціонованого доступу та використання. Для прикладу, отримавши банківську картку та знаючи її пароль, стає можливим проведення різного роду операцій з нею.

Попри всі методи захисту, найдостовірнішим фактором автентифікації і отримання різного роду привілеїв залишаються біометричні дані людини. Адже саме ці дані є найунікальнішими та майже не піддаються підробці. Такі елементи захисту застосовуються в сучасних автоматичних системах, таких як FaceID, сканер сітківки ока (іридосканер), відбиток пальця та структура ДНК. Оскільки такі технології ще не зовсім досконалі та мають певні технічні недоліки, їх використання в системах, де циркулює персональна інформація, є дуже складним та проблематичним. Тому основним і кінцевим фактором обробки інформації є людина [8].

Найсучасніші досягнення в системах ідентифікації та автентифікації пластикових документів безперечно пов'язані з використанням чипів. Головним чином через те, що такий спосіб дозволяє оцифровувати персональні дані, краще захистити процес автентифікації та зробити його достатньо швидким. Використання таких технологій є досить недешевим, а процес відтворення – складним. Через що не завжди виникає доцільність їх використання в окремих видах пропускних систем, що надають доступ до тих чи інших об'єктів за посвідченнями учасників різного роду організацій.

Тому, в цьому випадку, необхідно звернути увагу на використання старих, але значно покращених машинозчитуваних елементів.

Метою статті є аналіз пластикових документів (карток) з машинозчитуваними елементами захисту, вибір відповідного елементу персоналізації і його захисту та розробка аналогу системи автентифікації користувачів.

Виклад основного матеріалу

Було проаналізовано найбільш розповсюджені електронні елементи захисту пластикових карток: види, технології виготовлення, принцип роботи.

Магнітна смуга – носій інформації з обмеженим обсягом пам'яті.

Смуга може бути виготовлена для різних напруженостей магнітного поля. Кодування магнітної смуги виконується на спеціальному пристрої (енкодері), який дозволяє записати на неї інформацію, необхідну для подальшої роботи.

Подібні пластикові картки широко використовуються в платіжних і дисконтних системах, дуже рідко – в системах доступу.

Необхідно зазначити, що за кордоном магнітні картки застосовуються в системах контролю й управління доступом значно ширше внаслідок того, що впровадження даних систем на Заході почалося набагато раніше, ніж в Україні.

Кодування Smart-чипів також здійснюється спеціалізованими енкодерами, які, як і енкодери магнітних карток, можуть бути вбудовані в деякі моделі принтерів для їх виготовлення. Існує відмінність у напруженості магнітного поля: LoCo (Low Coercitive – низькокоерцитивні = 300 ерстед) і HiCo (High Coercitive – висококоерцитивні = 2750 ерстед) магнітні смуги.

Пластикові картки з магнітною смугою HiCo надійніші і довговічніші, оскільки інформація на магнітних смугах HiCo менш схильна до розмагнічення зовнішніми магнітними полями, ніж на смугах LoCo.

Магнітна смуга HiCo використовується в тих випадках, коли потрібно захистити інформацію на магнітній карті від можливого розмагнічування, а також підвищити захищеність карток від можливої підробки. Картки з магнітною смугою HiCo коштують дорожче, ніж картки з магнітною смугою LoCo.

Штрих-коди. Всі штрих-коди поділяються на лінійні (1D) та двомірні (2D). Лінійний штрих-код читається тільки в одному напрямку (перпендикулярно чорним лініям штрих-коду), а двомірний зчитується при будь-якому положенні.

Лінійні коди – це послідовність паралельних чорних та білих смуг різної ширини. Темні смуги називаються штрихами, а світлі – пробілами. Інформацію несе суворо задана стандартизована ширина штрихів та пробілів, а також їх розташування відносно один одного. Двомірний код містить інформацію як по горизонталі, так і по вертикалі.

Серед **чипів та міток,** в основу яких покладено використання бездротових (wireless) технологій, найбільш поширені наступні.

NFC означає комунікацію ближнього радіусу дії, RFID – радіочастотну ідентифікацію. Обидві технології використовують радіосигнал для пошуку тегів і відстеження цілей та приходять на зміну штрих-кодуванню. NFC тільки зароджується, а RFID вже поширена в усьому світі. RFID мітки (теги) містять антену і чип, в якому зберігаються дані.

Щоб побачити дані, потрібно RFID зчитувач. RFID часто працює на великих відстанях, інакше довелося б небезпечно міняти розташування, наприклад, при парковці автомобіля, до воріт, щоб переконатися що мітку дійсно зчитано рідером.

Як приклад, RFID – це система односпрямованого зв'язку, в якій дані з мітки передаються до безконтактного зчитувача.

Технологія NFC набагато менша версії RFID. Радіус її дії становить максимум 10 см і в ній може бути встановлений як односторонній, так і двосторонній зв'язок.

Розглянемо односторонню передачу даних.

Використовуючи смартфон, можна прочитати NFC тег, який може бути вбудований в рекламні постери, політичні листівки, путівники. Розумні мітки дуже схожі на RFID теги, вони просто налаштовані на роботу з NFC зчитувачами, замість RFID. RFID однонаправлена технологія, де зчитувач читає інформацію з мітки. NFC технології більш комплексні.

Як правило, кількість витрачених ресурсів та зусиль для захисту тієї чи іншої (інформації) системи залежить від рівня важливості даної системи.

Вартість виготовлення пластикових карток може бути різною.

У таблиці 1 наведено середню кількість витрат на їх виготовлення з тим чи іншим елементом захисту, тиражем в 100 штук. Для порівняння додано поліграфічні елементи захисту – ембосування і нумерацію [18].

Таблиця 1

Витрати на виготовлення пластикових карток

Елемент захисту на картці	Середня ціна, 100 шт.
Штрих-код	480 грн
Магнітна смуга	590 грн
Безконтактний чип	1200 грн
Ембосування	510 грн
Нумерація	480 грн

З таблиці добре видно, що найдорожчим з усіх запропонованих варіантів є виготовлення пластикової картки з безконтактним чипом. А варіант з виготовлення картки з QR-кодом є найдешевшим.

Усе це можна пояснити тим, що QR-код – це лише нанесене на поверхню зображення з використанням одного з видів друку, воно не вимагає значних витрат під час виробництва та використання.

Чип, навпаки, потребує застосування спеціалізованого обладнання для монтажу, а процедура його створення сама по собі є досить складною.

Ще однією, схожою з чипом, перевагою QR-коду є швидкість процедури його зчитування, адже навіть назва дає зрозуміти, що QR-код (англ. Quick Response Code) – це код швидкого реагування.

Поряд з перевагами QR-код має ряд недоліків.

Однією з найголовніших проблем використання QR-коду, як надійного елементу в процесі ідентифікації та автентифікації, є те, що процес та алгоритми його кодування та зчитування знаходяться в публічному доступі та є відомими [11].

Наступним недоліком є обмеження в кількості кодованих символів.

З аналізу та дослідження зібраного матеріалу випливає необхідність в кодуванні тієї інформації, за допомогою якої генерується QR-код. Мета цього кодування – приховати інформацію про об'єкт від зловмисника. Для вирішення цієї задачі потрібно використати елементи криптології [13; 14].

Тому було запропоновано процес хешування. Хеш-сумою (хешем, хеш-образом, хеш-кодом) називається значення хеш-функції на якихось вхідних даних. Іноді хеш-суму також називають дайджестом повідомлення. Значення хеш-суми може використовуватися для перевірки цілісності даних, їх ідентифікації та пошуку (наприклад в p2p-мережах), а також заміняти собою дані, які небезпечно зберігати в явному вигляді.

Саме такими даними є персональні відомості про об'єкт, а в нашому випадку це дані про особу. Криптографічна хеш-функція дозволяє легко перевірити, що деякі вхідні дані зіставляються із заданим значенням хешу, але, якщо вхідні дані невідомі, то навмисно важко відновити вхідне значення (або еквівалентну альтернативу), знаючи збережене значення хеш-функції. Це використовується для забезпечення цілісності переданих даних і є будівельним блоком для хеш-кодів аутентифікації повідомлень (HMAC), які забезпечують їх автентичність.

Явне значення хеш-суми, як правило, записується в шістнадцятковому вигляді. Так, утиліта md5sum, яка обчислює значення хеш-функції MD5 від заданого файлу, видає результат у вигляді рядка з 32-х шістнадцяткових цифр – наприклад, 026f8e459c8f89ef75fa7a78265a0025.

Однак, існує проблема, якої неможливо уникнути – це алгоритми хешування. Тобто, той факт, що хеші є рядком фіксованої довжини, означає, що для кожного введення даних є інші можливі входи, які приведуть до того ж хешу. Це означає, що якщо зловмисник може створювати ситуацію, він може передавати шкідливі файли чи дані та ховатися під правильним хешем.

Мета хорошої хеш-функції полягає в тому, щоб зробити надзвичайно складними для зловмисників способи генерації вхідних даних, які хешуються з однаковим значенням. Обчислення хеша не повинно бути занадто простим, так як це полегшує зловмисникам штучне обчислення.

Алгоритми хешування повинні бути стійкі до «атак знаходження прообразу». Тобто, щоб отримуючи хеш, було б надзвичайно складно обчислити зворотні детерміновані кроки, зроблені для відтворення значення, яке створило хеш.

З аналізу та дослідження опрацьованого матеріалу було визначено, що процес автентифікації має певні вимоги згідно з низкою керівних документів. Головним чином вимоги, що забезпечують автентичність документа, – це контроль доступу до системи (мережі) та створення процедури пасивноїй активної автентифікації.

Першочерговими та вже добре відомими способами захисту інформації у корпоративній мережі є встановлення надійних паролів, наявність резервних копій, безпечне використання додатків, оновлення системи та зміна налаштувань за замовчуванням.

Поряд з цим, особливу увагу під час забезпечення безпеки корпоративної мережі слід приділити захисту баз даних. Оскільки інформація, яку вони містять, особливо цінна для організацій та приваблива для зловмисників. Бази даних потребують особливої уваги та додаткового захисту [15].

Було опрацьовано питання щодо захисту баз даних. Проаналізовано інформацію компанії ESET – міжнародного розробника антивірусного програмного забезпечення та рішень в області комп'ютерної безпеки.

Спеціалісти ESET надають декілька основних порад щодо захисту баз даних підприємств і організацій.

1. *Контроль доступу до бази даних*. Запобігти атакам кіберзлочинців допоможуть обмеження дозволів та привілеїв. Крім базових системних дозволів слід застосувати:

Обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією.

Обмеження використання основних процедур тільки певними користувачами.

Уникнення використання і доступу до баз даних в неробочий час.

2. *Визначення критично важливих даних.* Першим кроком має стати аналіз важливості захисту для конкретної інформації. Для полегшення визначення місця та способу збереження конфіденційних даних слід зрозуміти логіку й архітектуру бази даних. Не всі дані є критично важливими чи потребують захисту, тому на них немає сенсу витрачати час і ресурси.

3. *Шифрування інформації*. Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації.

У разі використання уразливості або отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти бази даних, які, зазвичай, містять багато цінної інформації. Кращий спосіб захистити базу даних – зашифрувати її для осіб, які намагаються отримати доступ без авторизації.

4. *Реалізація анонімності непродуктивних баз даних*. Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проєкту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію.

Тобто за допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що й оригінал, але зі зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату.

Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати залежать від вибору адміністратора, але незалежно від вибору метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотної інженерії.

Цей метод рекомендовано використовувати для баз даних, які є частиною середовища тестування і розробки, оскільки він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

5. *Моніторинг активності баз даних*. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким.

Взявши до уваги цю інформацію, для ідентифікації було запропоновано використання алгоритму SHA3 для створення персонального QR-коду на основі текстових або інших, наприклад, біометричних, даних людини.

Даний QR буде унікальним посиланням на комірку пам’яті в системі та виконуватиме роль об’єкта безпеки системи. Головне завдання цього QR-коду – передати унікальність об’єкта (людини) для машинозчитувальних систем.

Створення хеш-суми відбувається за допомогою спеціального додатку divHasher. Це невелика програма, що працює під Windows, призначена для зручного і надзвичайно швидкого обчислення хешів (або контрольних сум) для будь-яких файлів або тексту. Утиліта вміє підраховувати контрольні суми практично за всіма поширеними алгоритмами: MD2, MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-128, RIPEMD-160, RIPEMD-256, WHIRLPOOL, Tiger , Adler32, CRC32 і Panama.

Для використання програми необхідно вибрати файл або вставити в спеціальне віконце текст, контрольні суми яких потрібно розрахувати.

Далі вибирають алгоритми і натискають кнопку «Обчислити». Після підрахунку можна скопіювати будь-які дані в буфер обміну прямо з програми. Приклад обчислення даних наведено на рис. 1.

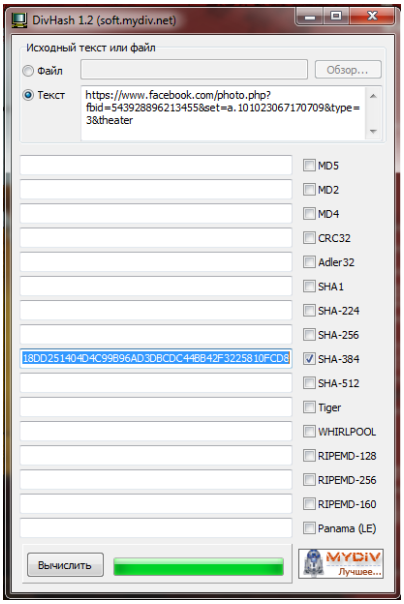

Рис. 1. Приклад отримання хеш-суми завдяки алгоритму SHA3

У запропонованому прикладі хешуються персональні дані, такі як ПІБ, дата та місце народження, місце навчання (роботи, служби), ідентифікаційний номер. Додатково можна використовувати відповіді на запитання.

Далі генеруємо QR-код за допомогою спеціального додатку QR-Code Studio. QR-Code Studio – Дизайнер QR-Code – безкоштовна програма для швидкого та легкого створення QR-кодів. Програма дуже проста у використанні і не вимагає ніяких спеціальних знань. Помічник введення даних спрощує створення штрих-кодів QR-Code для мобільного маркування та маркетингу: всього за кілька секунд можна створити штрих-коди QR-Code для вебсайтів, скачування файлів, для посилань на додатки, Facebook, Twitter і LinkedIn сторінки, SEPA-платежі, відправки SMS.

Створені QR-Code штрих-коди можуть бути збережені у форматі растрової графіки (BMP, GIF, JPG, TIF, PNG) або скопійовані в буфер обміну.

Отримані зображення поширюються за ліцензією Royalty Free і можуть бути використані або оброблені для цілей приватного чи некомерційного використання.

Крім цього, підтримується створення електронних бізнес-карток в форматах vCard або meCard. Приклад генерації наведено на рис. 2.

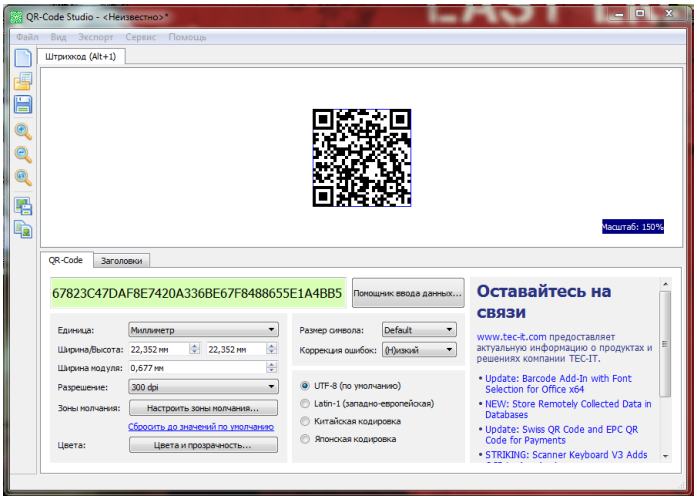

Рис. 2. Генерування QR-коду з даних у вигляді хеш суми

В подальшому даний QR-код можна застосовувати на пластиковому документі, комбінуючи його з іншими елементами захисту. Однак це не обов’язково, адже в процесі автентифікації буде представлено всі дані про об’єкт, якому належить цей код.

Практична реалізація процедури автентифікації

Контроль доступу в запропонованому алгоритмі реалізується шляхом захищеності процедури доступу до всіх груп даних, що містяться в системі. Приклад структури бази даних зображено в таблиці 2. Застосування об’єкта системи та захищеність її бази даних від несанкціонованого доступу відіграє роль активної та пасивної автентифікації в даному алгоритмі. Далі, після зчитування QR-коду, персональні дані графічно виводяться на пристрій. Це надає змогу вповноваженій особі чи системі отримати та порівняти потрібну персоналізовану інформацію про людину, щоб підтвердити її статус.

Таблиця 2

Структура бази даних

Хеш-сума	Об’єкт системи
026f8e459c8f89ef75fa7a78265a0025	file 1425.jpg
ef75fa7a78265a0025026f8e459c8f89	file 2467.jpg

Дану систему можна реалізувати на апаратній частині у вигляді спеціалізованого ліцензійного додатку для різних операційних систем (android, IOS, Windows, Linux та ін.). А також є варіант створення спеціального вебсервера баз даних.

Сервер баз даних виконує обслуговування та управління базою даних та відповідає за цілісність та збереження даних, а також забезпечує операції введення-виведення при доступі клієнта до інформації. Архітектура клієнт – сервер складається з клієнтів та серверів. Основна ідея полягає в тому, щоб розміщувати сервери на потужних машинах, а додаткам, що використовують мовні компоненти системи контролю і управління доступом, забезпечити доступ до них з менш потужних машин-клієнтів за допомогою зовнішніх інтерфейсів.

Дана система дозволяє відмовитись від елементів персоналізації на самій картці, адже всі персоналізовані дані тепер зберігаються в захищеній базі даних системи. Це дозволить значно здешевити процес створення ідентифікаційного документу. Однак необхідне чітке розмежування в доступі різних класів користувачів. Наприклад, супер-користувач – співробітник організації (установи), який наділений правами щодо втручання та допуску до бази даних може додавати та видаляти учасників системи. Адміністратор – співробітник, який використовує базу даних для службових цілей, але не має можливості зміни або втручання в роботу бази даних. Та учасник системи – фізична особа, яка лише користується системою для отримання допуску до об’єкта або привілеїв, пов’язаних з цим об’єктом.

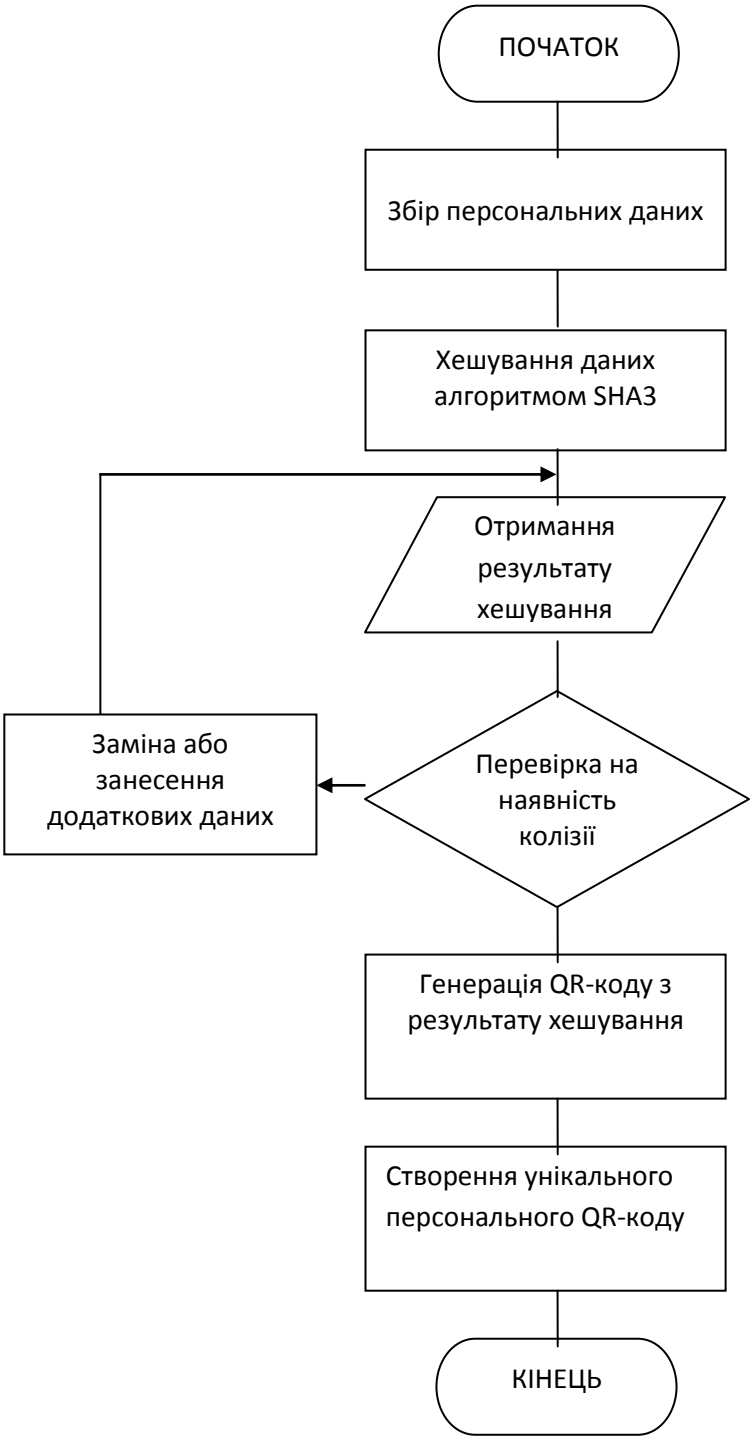

Рис. 3. Блок-схема алгоритму ідентифікації та створення персонального QR-коду

Практичне застосування

Використовуючи алгоритм ідентифікації, хешуємо дані у вигляді вебпосилання (URL), як приклад використовується персональна сторінка з соцмережі facebook (рис. 1). Також необхідно перевірити, чи не відбулась невідповідність в процесі хешування інформації. Відомості чи сукупність відомостей про фізичну особу, в тому числі фото, статус, рід занять, дозволять здійснити перевірку дійсності документа та відповідність його власнику. В подальшому є можливість створити спеціальний захищений вебсервер для обробки, зберігання та використання персональної інформації членів установи або організації.

Далі генеруємо QR-код з хеш-суми (URL). Таким чином інформація про дані у вигляді вебпосилання приховується, а залишається лише набір символів. Для реалізації процедури

автентифікації розроблено спеціальний додаток faceScanQr для смартфонів з операційною системою Android. Цей додаток має вбудовану базу даних з можливістю запису та видалення з неї інформації. Також в програму вбудовано елемент, який зчитує 2D (QR) коди. Інформація подається у вигляді ключа та вебпосилання (URL), далі вони заносяться в базу даних інстальованого додатку (рис. 4).

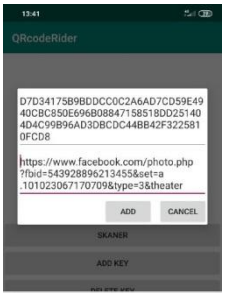

Рис. 4. Занесення інформації в базу даних

Рис. 5. Блок-схема алгоритму автентифікації та підтвердження статусу

Процес роботи можна описати, використовуючи змінні Н, у, та х. Де Н – це об’єкт бази даних (рядок в таблиці), х – це ключ (код), у – посилання, де х=у. При зчитуванні сканером ключа на екран виводиться лише у. Тобто реалізується система, де наявні публічні та приватні дані (рис. 6).

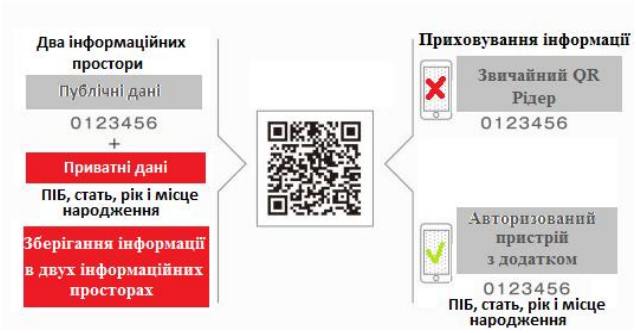

Рис. 6. Принцип дії системи

Рис. 7. Блок-схема алгоритму роботи додатку faceScanQr

Висновки. Аналіз сучасних пластикових документів, ступенів їх захисту, елементів ідентифікації та автентифікації показав, що найголовнішим методом забезпечення процесу ідентифікації та автентифікації пластикових документів виступає реалізація в процесі

створення систем на основі машинозчитуваних елементів. Кожен вид машинозчитуваного елементу має власну технологію створення і відповідні властивості. Залежно від цих властивостей підбирається варіант застосування елементу в пластикових документах різного рівня важливості.

Встановлено, що на ступінь захищеності документа впливають два основні чинники, такі як контроль доступу та проведення кінцевих пасивної або активної автентифікацій.

Розроблено власний варіант системи ідентифікації та автентифікації пластикових документів на основі 2D (QR) коду.

Запропонована система може бути використана як аналог більш дорогим варіантам організації контрольно-пропускного режиму на об'єктах завдяки своїй простоті, малоймовірності несанкціонованого доступу до алгоритмів і процесу роботи її елементів.

Використання даної системи на контрольно-пропускних пунктах може значно покращити управління та забезпечити захищеність системи безпеки, процесу перетину контрольованої зони. Підсумовуючи результати, можна стверджувати: щоб якісно та надійно захистити документ від підробки, забезпечити його автентичність – необхідно надалі покращувати процеси кодування, ідентифікації та автентифікації персоналізованої інформації. Напрямком подальших досліджень може бути розробка системи з переносом персоналізованої інформації з документів напряму до баз даних машинозчитуваних систем. Адже, по-перше, це захистить персональну інформацію особи від дій зловмисника. По-друге, це полегшить сам процес створення документів і значно здешевить його. Однак найважливішим параметром залишиться стійкість та захищеність від несанкціонованого втручання в роботу машинозчитуваних електронних систем.

ЛІТЕРАТУРА

1. Вольфган Р., Вольфганг Е. Довідник зі смарт-карток. *Довідник* / John Wiley & Sons. 4 листопада 2010 р. Технологія та інженерія. 1088 с.

2. ДСТУ ISO–7810. ID-картки – фізичні характеристики.

3. ДСТУ ISO 7811. ID-картки – методи запису.

4. ДСТУ ISO–7812. ID-картки – система нумерації і процедура реєстрації ідентифікаторів емітентів (5 частин).

5. ДСТУ ISO–7813. ID-картки – картки для фінансових транзакцій.

6. ДСТУ ISO–7816. ID-картки – картки з мікросхемою і контактами (6 частин).

7. Абакумов В. Г. Методи захисту пластикових карт / В. Г. Абакумов, Л. В. Ратомська // Друга конференція молодих вчених «Електроніка – 2009»: збірник статей. Київ, 2009. Ч. 2. С. 61–68.

8. Пиріг С. О. Платіжні системи: навч. посіб. Київ: Центр учбової літератури, 2008. 240 с.

9. Бугаєв Леонід. Мобільний маркетинг. Як зарядити свій бізнес в мобільному світі. Москва: Паблішер, 2012. 214 с. ISBN 978-5-9614-2222.

10. ДСТУ ISO / IEC 18004-2015. Інформаційні технології. Технології автоматичної ідентифікації та збору даних. Специфікація символіки штрихового коду QR Code.

11. Проведення судово-технічної експертизи документів, оснащених машинозчитуваними елементами захисту: метод. рек. / Мін'юст України; за ред. Л. М. Головченко. Київ: КНДІСЕ, 2012. 95 с.

12. Шнайер Брюс. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Сі. Москва: Тріумф, 2002. ISBN 5-89392-055-4.

13. Дональд Кнут. Мистецтво програмування. (The Art of Computer Programming). 2-ге вид. Москва: Вільямс, 2007. Том 3. Сортування і пошук (Vol. 3. Sorting and Searching). 824 с. ISBN 0-201-89685-0.

14. Вірт Ніклаус. Алгоритми і структури даних. Москва: Мир, 1989. ISBN 5- 03-001045-9.

15. Киричок П. О. Захист цінних паперів та документів суворого обліку. Київ: НТУУ «КПІ», 2008. 368 с.

УДК 621.391

канд. техн. наук Радзівілов Г. Д. (ВІТІ)
Цатурян О. Г. (ВІТІ)
канд. техн. наук Бєляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ)
Цимбал І. В. (ВІТІ)

ЧАСТОТНО НЕСЕЛЕКТИВНИЙ ПРОСТОРОВИЙ КАНАЛ З ВИКОРИСТАННЯМ АДАПТИВНИХ АНТЕННИХ РЕШІТОК

Просторова обробка сигналів в адаптивних антенних решітках повинна забезпечувати оптимальний прийом сигналу від деякого заданого джерела, для цього необхідна максимізація відношення сигнал – шум на вході адаптивних антенних решіток. Дане завдання добре вивчене для випадку, коли джерело сигналу є нерухомим і точковим, а для мобільних об'єктів часто доводиться застосовувати складні алгоритми управління адаптивними антенними решітками. Результат наукового дослідження показав, що одним із найбільш перспективних підходів вирішення задачі, що підкреслює актуальність, є підвищення ефективності прийому сигналу при використанні адаптивних антенних решіток і відповідних методів просторової обробки сигналів. Тому, в основу пропонується застосувати оптимальний метод обробки сигналів, що покладено в основу Recursive Least Squeare алгоритмів, який дозволяє забезпечити вимоги до обчислювальної складності і відношення сигнал/шум.

У реальному каналі зв'язку передбачається наявність кутової дисперсії сигналу через його багатопроменеве поширення. Конфігурація адаптивних антенних решіток передбачається довільною. Удосконалений метод адаптивного прийому сигналів від рухомих джерел дозволяє знизити обсяг обчислень порівняно з існуючим, коли ваговий вектор з адаптивними антенними решітками є оптимальним і вибирається як власний вектор сигнальної кореляційної матриці, що визначає його новизну, при цьому можливо забезпечити досить високу ефективність прийому сигналів. Показано, що застосування запропонованого удосконаленого методу забезпечує складність $\sim N^2$ *, що на порядок нижча ніж при використанні існуючого оптимального методу.*

Ключові слова: *адаптивна антенна решітка, кореляційна матриця сигналу, просторова обробка сигналів, адаптивний прийом сигналів.*

H. Radzivilov, O. Tsaturyan, R. Beliakov, I. Tsymbal. The method of adaptive signal reception with adaptive antenna arrays from moving sources.

Spatial signal processing in adaptive antenna arrays should provide optimal signal reception from some desired source, this requires maximizing the signal-to-noise ratio at the output of adaptive antenna arrays. This task is well studied for the case when the signal source is fixed and point, and for mobile objects often have to use complex algorithms for controlling adaptive antenna arrays. The relevance of this study is that one of the most promising approaches to solving the problem is to increase the efficiency of signal reception is the use of adaptive antenna arrays and appropriate methods of spatial signal processing.

The angular dispersion of the signal is assumed to be due to its multipath propagation in the communication channel. The configuration of adaptive antenna arrays is assumed to be arbitrary. This method allows to reduce the amount of calculations compared to the method when the weight vector with adaptive antenna arrays is optimal and is selected as the eigenvector of the signal correlation matrix and it is possible to maintain the efficiency of the signal is quite high, which determines its novelty.

The article analyzes the method of adaptive reception of signals from moving sources using adaptive antenna arrays which is also called the method of quasi-optimal signal processing received by adaptive antenna arrays from a moving source with unknown angular coordinates, the possibility of its reception by mobile subscribers in angular variance. quasi-optimal signal processing with other known methods of signal processing.

Keywords: *adaptive antenna array, signal correlation matrix, gender basis, spatial signal processing, adaptive signal reception.*

Вступ. Забезпечення основних вимог до систем радіозв'язку (далі – СРЗ) на базі рухомих об'єктів – забезпечення якісного радіозв'язку, оперативної доставки інформаційних потоків заданої якості із забезпеченням необхідного рівня захисту інформації вимагає синтезу багатьох інфокомунікаційних способів удосконалення цих систем.

В даний час спостерігається інтенсивний розвиток СРЗ (системи зв'язку з рухомими об'єктами), найважливішим напрямком досліджень в даній області є підвищення ефективності прийому сигналу. Одним з найбільш перспективних підходів до вирішення даної проблеми є використання адаптивних антенних решіток (далі – ААР) і відповідних методів просторової обробки сигналів [1]. Застосування ААР дозволяє підвищити вихідне відношення потужності сигналу до середньої потужності шуму (далі – ВСШ), забезпечити боротьбу з глибокими завмираннями (федінгами) сигналу та збільшити число одночасно обслуговуваних користувачів за рахунок їх просторового розподілу. Просторова обробка сигналів в ААР повинна

забезпечувати оптимальний прийом сигналу від деякого бажаного джерела і, як правило, для цього потрібно максимізація ВСШ на виході ААР. Дана проблема добре вивчена для випадку, коли джерело сигналу є нерухомим і точковим [1]. Однак на практиці це припущення часто неможливе. Так, для багатопроменевого каналу зв'язку, коли сигнал зазнає множинні відображення і являє собою суперпозицію плоских хвиль, характерна кутова дисперсія сигналу. Тому його просторовий (кутовий) спектр може значно розширюватися і бути невідомим. Наприклад, в дослідженні [1] розглядались особливості прийому сигналу з кутовою дисперсією. У них також передбачалося, що джерело залишається нерухомим. Більш того, в роботах з адаптивної обробки сигналів в ААР часто передбачається, що координати джерела сигналу відомі і використовуються для завдання вектора корисного сигналу [1]. Насправді в системах мобільного зв'язку джерело сигналу знаходиться в русі, і тому його положення слід вважати невідомим або відомим з великою похибкою (наприклад, апріорі може бути заданий тільки кутовий сектор розташування абонента). Невідомою буде також і кутова дисперсія сигналу, якщо канал зв'язку є багатопроменевим. Щоб врахувати апріорну невизначеність параметрів сигналу, необхідно застосовувати адаптивні методи його обробки. Ефективність адаптивної обробки сигналу, прийнятого від нерухомого джерела, збільшується, якщо зростає час адаптації. Однак для рухомого джерела час адаптації не може бути обраний скільки завгодно великим, тобто необхідно обирати компромісний варіант. Таким чином, для заданої швидкості джерела існує деякий оптимальний час адаптації, при якому ефективність обробки є найкращою.

Аналіз наукових праць предметної області. У роботі [2] розкрито методику підвищення швидкодії та динамічної точності систем управління діаграмою направленості ААР, із використанням методів компенсації внутрішніх середньоквадратичних помилок системи діаграмоутворення. У роботі [4] розкрито метод вимірювання співвідношення сигнал/шум з метою забезпечення адаптивного виділення оптимального каналу прийому. Зокрема, у роботі [5] показано ряд напрямів удосконалення способів підвищення ВСШ за рахунок оптимального діаграмоутворення ААР з використанням алгоритмів просторово-часової фільтрації та маршрутизації інформаційних потоків.

Переваги та недоліки алгоритмів адаптивної фільтрації сигналу, зокрема, що впливають на час адаптації, були проаналізовані в [2], а саме:

Перевага алгоритму Least Means Square (LMS) полягає у низькій обчислювальній складності. Основним недоліком алгоритму LMS є повільна збіжність і підвищена дисперсія помилки в сталому режимі. На практиці застосування таких алгоритмів призводить до збільшення рівня вихідного шуму, що є неприйнятним у випадку формування вузького променя ААР, тому в подальшому в статті цей алгоритм розглядатися не буде. Головною перевагою використання алгоритмів Recursive Least Squares (RLS) та алгоритму на основі Калмановської фільтрації є можливість забезпечення кращої стійкості системи адаптивної фільтрації, проте в умовах перехідних процесів переналагодження ААР із великою кількістю елементів збільшується обчислювальна складність [5], що вимагає накладання обмежень щодо кількості модулів ААР.

Метою статті є аналіз адаптивного прийому просторово розподілених сигналів від рухомих джерел на тлі власних шумів приймальних пристроїв в умовах частотно-неселективного просторового каналу. Завданням є визначення вагового вектора, який забезпечує близьке до максимального ВСШ на виході ААР. Досліджується вплив часу адаптації на величину вихідного ВСШ. Представлено схема адаптивної обробки сигналу з використанням удосконаленого методу.

Виклад основного матеріалу. Припустимо, що ААР з N елементів приймає сигнал з кутовою дисперсією. Тоді величина вихідного ВСШ представлена у вигляді [3]:

$$\rho(W) = \frac{W^H MsW}{\sigma^2 W^H W}, \tag{1}$$

де Ms – кореляційна матриця корисного сигналу в приймальних каналах ААР;

σ_n^2 – дисперсія власного шуму в одному елементі, яку далі без втрати спільності будемо вважати одиничної $\sigma_n^2 = 1$;

W – ваговий вектор обробки сигналу.

Максимум величини вихідного ВСШ (1) спостерігається при ваговому векторі W, що дорівнює власному вектору U_1, відповідному максимальному власному числу λ_1 кореляційної матриці сигналу Ms [1]. Даний метод має гарну ефективність, але вимагає значних обчислювальних витрат, що є критичним параметром в системах реального часу. Тому, в основу пропонується застосувати оптимальний метод обробки сигналів, що покладено в основу RLS алгоритмів [9], який дозволяє забезпечити вимоги до обчислювальної складності. Ваговий вектор W в цьому випадку задається у наступному вигляді:

$$W = \beta_0 S_0 + \beta_1 M S_0 + \beta_1 M^2 S_0 + ... + \beta_{N-1} M^{N-1} S_0, \quad (2)$$

де матриця $M = \langle XX^H \rangle = M_S + I$ є сумою кореляційної матриці сигналу Ms і власного шуму I;

X – вектор вхідного сигналу ААР;

вектори $S_0, MS_0, M^2 S_0, ... M^{N-1} S_0$ – ступеневі вектори [9];

β_i – коефіцієнти розкладання; кутові дужки позначають статистичне усереднення.

Щоб скористатися цим виразом для формування вагового вектора, необхідно знати матрицю M і вибрати вихідний вектор S_0. У разі невідомого положення джерела сигналу матрицю M можна виміряти, використовуючи вибірки вектора вхідного сигналу X, а за вихідний вектор доцільно вибрати один із стовпців кореляційної матриці сигналу M.

Для доведення, що така обробка сигналу може бути ефективною для рухомого джерела, розглянемо точкове джерело, яке створює в апертурі ААР розподіл сигналу у вигляді вектора Φ з нормою $\Phi^H \Phi = N$, де верхній індекс H позначає ермітове спряження. В цьому випадку $M = \nu \Phi^H \Phi + I$ [2], де ν – величина ВСШ в одному елементі ААР. Легко перевірити, що вектор Φ є власним для матриць Ms і M. Виберемо його в якості вагового вектора, тобто $W = \Phi$, і підставимо в (1). В результаті отримаємо максимально можливе вихідне ВСШ, що дорівнює νN. Отримано результат, коли ВСШ на виході ААР більше в N раз, ніж ВСШ на вході в одному елементі. Далі припустимо, що положення джерела сигналу невідоме і вектор Φ також є невідомим. Виберемо довільний стовпець M_j матриці M. Він є кореляційним вектором, тобто $M_J = X_{xj} \Phi + I_j$, де I_j – стовпець одиничної матриці I з номером j. Таким чином, вектор M_j відрізняється за нормою від власного вектора Φ матриці M_S на величину $(\nu N)^{-1}$. На практиці вихідне ВСШ νN має бути велике, тому можна вважати, що $\nu N \geq 10$. Звідси випливає, що кореляційний вектор M_j мало відрізняється від власного вектора Φ і може бути наближено прийнятий як ваговий вектор W. Такий підхід до адаптивної обробки дає високу ефективність і для джерел сигналу з кутовою протяжністю. Ефективність прийому збільшується, якщо число членів в розкладанні (2) збільшується. При цьому за вихідний вектор S_0 рекомендується вибирати один з центральних стовпців матриці M_j для того, щоб виключити втрати в підсиленні антени через несиметричний амплітудний розподіл у ваговому векторі. Схема обробки сигналу в ААР з ваговим вектором у вигляді кореляційного вектора $M_j = \langle X x_j^* \rangle$ представлена на рисунку 1.

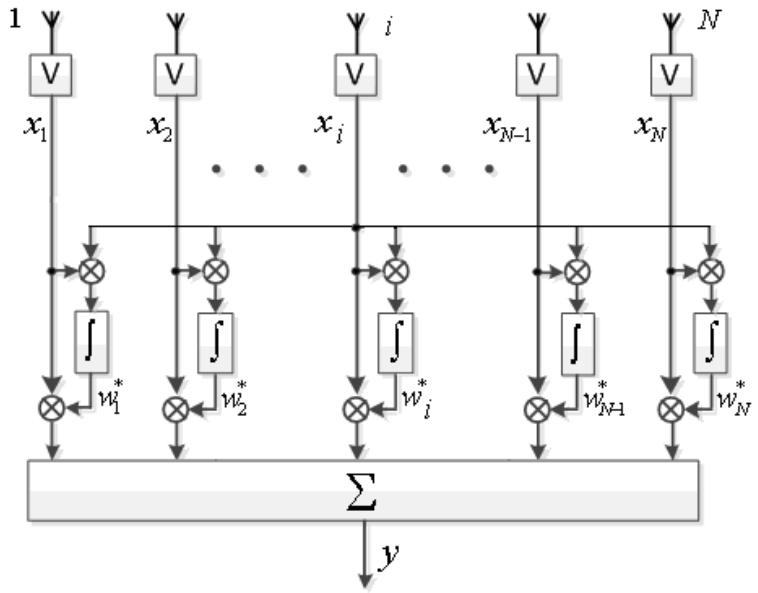

Рис. 1. Схема обробки сигналу в ААР

Результати моделювання. Максимально правдоподібна оцінка кореляційної матриці M за критерієм максимальної правдоподібності по L вибірках вхідного процесу має вигляд:

$$\overline{M} = \frac{1}{L}\sum_{l-1}^{L}(l)x(l)x^{H}(l) \tag{3}$$

Так, для нерухомого джерела при достатньо великій довжині вибірки оціночна кореляційна матриця $\overline{M}$ буде прагнути до дійсної кореляційної матриці M. Однак для випадку рухомого джерела дане твердження не буде справедливим. При великій довжині вибірки точність оцінювання почне падати, так як за час вимірювання джерело сигналу встигне переміститися на деякий кут щодо ААР. Тому для рухомих джерел вибір оптимальної кількості середньо-розрахованих параметрів буде залежати не тільки від числа елементів ААР і кутової ширини джерела, але і від його кутової швидкості. Для оцінки ефективності запропонованого удосконаленого методу адаптивного прийому сигналів від рухомих джерел була використана 3GPP-модель просторового каналу стільникового зв'язку для міських умов [1], в якій передбачається, що сигнал, який передається користувачем, відбивається від кластерів (великих об'єктів) і приходить на базову станцію у вигляді суперпозиції плоских хвиль з випадковими фазами. Число кластерів задається фіксованим і рівним шести. Просторовий спектр сигналу, відбитого від кожного кластера, являє собою розподіл Лапласа з шириною 2^{o} за рівнем половинної потужності і моделюється за допомогою двадцяти плоских хвиль однакової амплітуди із заданими кутами падіння. Кутове положення кластерів є випадковим для кожної реалізації багатопроменевого каналу і задається з умови, що середній просторовий спектр джерела має розподіл Лапласа з деякою шириною $\Delta\theta_s$ за рівнем половинної потужності. Тоді канальний коефіцієнт для *q*-го елемента АР можна записати у вигляді:

$$h_q = \sum_{n=1}^{6}\sqrt{\frac{P^H}{20}\sum_{m=1}^{20}\exp(jkd_q\sin(\theta_{nm}))\exp(j\Phi)} \tag{4}$$

де k – хвильове число;

d_q – відстань від *q*-го елемента ААР до початку обраної системи координат;

θ_{nm} – кут приходу *m*-й плоскої хвилі від *n*-го кластера;

θ_{nm} – фаза відповідного сигналу, рівномірно розподілена в інтервалі $[0 \div 2\pi]$;

P_n – потужність сигналу, відбитого від *n*-го кластера, яка є випадковою величиною.

При цьому загальна потужність P сигналу залишається постійною $(P_1 + P_2 + ... + P_6 = P)$. На рисунку 2 показана 3GPP-модель просторового каналу.

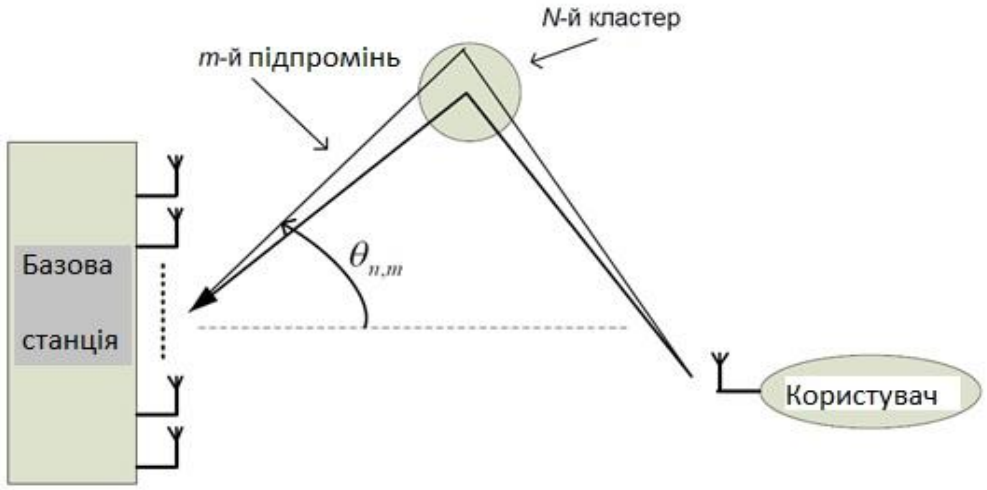

Рис. 2. GPP-модель просторового каналу

При моделюванні порівнювалася ефективність запропонованого удосконаленого методу з існуючим оптимальним методом прийому сигналу, коли за ваговий вектор застосовувався власний вектор вибіркової матриці (3). Для заданого розміру блоку L обчислювався оптимальний ваговий вектор і ваговий вектор, отриманий згідно з (2) при кількості членів розкладання, що дорівнює двом. Отримані вагові вектори використовувалися для прийому сигналу наступного блоку довжини L. На рисунку 3 представлені криві, що характеризують втрати Δp в ВСШ для оптимального й удосконаленого методів по відношенню до максимального ВСШ, отриманого при оптимальному прийомі з точно відомою кореляційної матрицею сигналу M . Результати наведені залежно від розміру блоку L, а також кутової швидкості джерела Ω щодо ААР. Рівень 0 дБ на графіках відповідає прийому сигналу з оптимальним ваговим вектором W_{opt} при точно відомій матриці M. Центральний кут приходу сигналу був рівномірно розподілений в інтервалі від -60^o до 60^o, а кількість усереднених дослідів було вибрано рівним 1000, що забезпечувало рознесення середнього значення ефективності менше, ніж 0,03 дБ. На рисунку 3 суцільною кривою позначені результати моделювання для оптимального вагового вектора, а пунктиром – для удосконаленого методу. Криві 1, 2 і 3 отримані для кутових швидкостей Ω, відповідно рівних 0,0025, 0,0050 і 0,0075 рад/T_s, де T_s – період проходження сигналів.

Як видно з графіків, втрати в ВСШ мають місце як при малій, так і при великій довжині вибірки L. Збільшення довжини вибірки спочатку веде до зростання ефективності обробки сигналу за рахунок зменшення помилки оцінювання кореляційної матриці, а потім ефективність знижується, так як помилка оцінювання кореляційної матриці збільшується через рух джерела сигналу. Таким чином, максимальна ефективність обробки сигналу спостерігається при деякій кінцевій довжині вибірки. Інший висновок полягає в тому, що запропонований удосконалений метод має суттєво менші втрати порівняно з оптимальним методом, що використовує власний вектор матриці (3) як ваговий вектор. Обчислювальну складність кожного методу можна оцінити загальною кількістю комплексних множників (КМ). Число КМ для запропонованого удосконаленого методу приблизно дорівнює $2NL + 5NL\ (p - 1)$, де p – число членів ряду (2), що використовуються для побудови вагового вектора. Число КМ, необхідне для обчислення власного вектора матриці (3), складає $\sim\left(N^2L + N^3\right)$ [1].

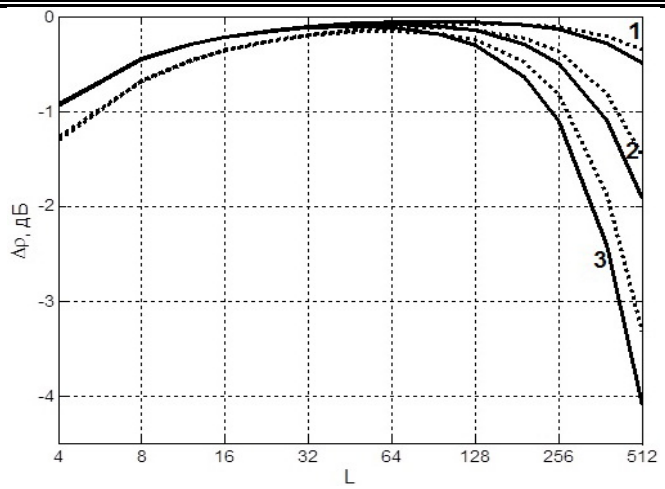

Рис. 3. Криві, що характеризують втрати Δp

Таким чином, для багатоелементних ААР $AP(N >> 1)$ і при довжині вхідного процесу, сумісною з числом елементів $AP(L \sim N)$, запропонований удосконалений метод має складність $\sim N^2$, в той час як оптимальний метод володіє складністю $\sim N^3$. наприклад, якщо $N = 16$ і $L = 32$, то адаптивний метод має виграш в обсязі обчислень в 12 і 4 рази при використанні нульового і першого наближення в (2) відповідно.

Висновки

1. Запропонований удосконалений оптимальний метод адаптивного прийому сигналів від рухомих джерел з використанням ААР забезпечує ефективність, близьку до максимально можливої.

2. Метод може бути використаний для прийому сигналів від мобільних абонентів в умовах обмежень що накладаються міськими перешкодами (будівлями, іншими спорудами), коли спостерігається кутова дисперсія сигналу, а також в системах супутникового й авіаційного зв'язку.

3. Порівняно з відомим оптимальним методом прийому сигналу даний метод має низьку обчислювальну складність, що важливо для практичного застосування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Джиган В. И. Адаптивная фильтрация сигналов: теория и алгоритмы / В. И. Джиган // Мир цифровой обработки. 2013.

2. Godara L. C. Smart Antennas / Godara L. C. // CRC Press. 2004. 472 p.

3. Умняшкин С. В Основы теории цифровой обработки сигналов: учебное пособие. Москва: ТЕХНОСФЕРА, 2019. 550 с.

4. Бєляков Р. О., Радзівілов Г. Д., Лебідь Є. В., Цатурян О. Г. Методика підвищення швидкодії та динамічної точності систем автоматичного керування діаграмою направленості АФАР [Текст] // Збірник наукових праць ВІТІ. 2015. № 1. С. 6–15.

5. Lee K.-A., Gan W.-S., Kuo S. M. Subband Adaptive Filtering: Theory and Implementation. UK, West Sussex: John Wiley and Sons, Ltd., 2009. 324 p.

6. Коуэн Ф. Н., Грант П. М. Адаптивные фильтры / Пер. с англ. Москва: Мир, 1988. 392 с.

7. Джиган В. И. Многоканальные RLS- и быстрые RLS-алгоритмы адаптивной фильтрации. Москва: Успехи современной радиоэлектроники, 2004. 482 с.

8. Шишацький А. В., Жук О. Г., Бєляков Р. О. Методика адаптивного управління параметрами MIMO-АФАР // Системи озброєння і військова техніка. 2016. № 4. С. 77–82.

9. Слюсар В. И. Основные понятия теории и техники антенн. Антенные системы евклидовой геометрии. Фрактальные антенны. SMART-антенны. Цифровые антенные решетки (ЦАР). MIMO-системы на базе ЦАР. Особенности построения суперлинейных усилителей. Москва: Техносфера, 2005. 569 с.

10. Бєляков Р. О., Мартинюк В. В., Лебідь Є. В., Цатурян О. Г. Аналіз алгоритмів адаптивної фільтрації сигналів в системах радіозв'язку // Збірник наукових праць ВІТІ. 2018. № 4. С. 132–140.

УДК 621.396

Ченченко В. А. ORCID: 0000-0003-1850-0508 (ВІТІ)
Руденко В. І. ORCID: 0000-0003-3563-5484 (ВІТІ)
Бондаренко Л. О. ORCID: 0000-0003-3563-5482 (ВІТІ)
Зінченко М. О. (ВІТІ)

АНАЛІЗ ЗАВАДОЗАХИЩЕНИХ РЕЖИМІВ РОБОТИ СУЧАСНИХ ВІЙСЬКОВИХ УКХ РАДІОСТАНЦІЙ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЇХ ВИКОРИСТАННЯ

На даний час в Збройних силах України організовані та функціонують УКХ радіомережі, побудовані в основному з використанням обладнання "Motorola", "Harris", "Aselsan". Основна проблема застосування засобів зв'язку "Motorola" – робота на фіксованих частотах, у достатньо вузькому діапазоні частот (136–174 МГц), що призводить до низької завадозахищеності ліній радіозв'язку. На відміну від обладнання "Motorola", в радіостанціях "Harris" та "Aselsan" реалізовані сучасні завадозахищені режими роботи, зокрема з псевдовипадковим переналаштуванням робочих частот (ППРЧ).

Досвід бойових дій у зоні проведення операції Об'єднаних сил (ООС) вказує на необхідність підвищення ефективності використання існуючих можливостей УКХ радіостанцій тактичної ланки управління. В умовах активної радіоелектронної протидії противника підвищення завадозахищеності ліній радіозв'язку набуває особливої актуальності і вимагає постійного вдосконалення засобів радіозв'язку на основі досягнень сучасної науки.

У дослідженні, на прикладі УКХ радіостанції тактичної ланки управління "Harris" RF-7850M-HH, проаналізовані наявні на сьогодні завадозахищені режими роботи та розроблені практичні рекомендації щодо їх використання в умовах впливу основних видів навмисних завад.

Викладені у статті практичні рекомендації можуть бути використані при розробці інструкцій щодо забезпечення функціонування УКХ радіостанцій тактичної ланки управління в умовах радіозавад.

V. Chenchenko, V. Rudenko, L. Bondarenko, M. Zinchenko. Analysis of interference-protected operating modes of modern military VHF radio stations of the tactical link of management and practical recommendations of recommendations.

At present, the Armed Forces of Ukraine have organized and operate VHF radio networks, built mainly using equipment "Motorola", "Harris", "Aselsan". The main problem with the use of "Motorola" communications is the operation at fixed frequencies, in a fairly narrow frequency range (136 - 174 MHz), which leads to low noise immunity of radio lines. Unlike Motorola equipment, "Harris" and "Aselsan" radios implement modern noise-tolerant modes, including with frequency hopping spectrum spreading (FHSS).

The experience of combat operations in the area of the Operation Joint Forces (OJF) indicates the need to increase the efficiency of the use of the existing VHF capabilities of tactical radio stations. In the conditions of active radio-electronic counteraction of the enemy, the increase of noise protection of radio communication lines becomes especially relevant and requires constant improvement of radio communication means on the basis of the achievements of modern science.

The study, on the example of VHF radio tactical control unit "Harris" RF-7850M-HH, analyzed the current noise-protected modes of operation and developed practical recommendations for their use in the face of major types of intentional interference.

The practical recommendations set out in the article can be used in the development of instructions for ensuring the operation of VHF radio stations of the tactical management in the conditions of radio interference.

Ключові слова: *завадозахищеність, режим роботи з ППРЧ, хопсет, швидкість передачі.*

Постановка завдання в загальному вигляді

Однією з основних характеристик систем радіозв'язку (СРЗ) є завадозахищеність, складовими якої є завадостійкість і скритність [1–4].

Одним з ефективних шляхів забезпечення завадозахищеності сучасних СРЗ в умовах впливу навмисних або ненавмисних завад є застосування сигналів з розширеним спектром: шумоподібних сигналів (ШПС), сигналів з псевдовипадковим переналаштуванням робочих частот (ППРЧ), псевдовипадковим переналаштуванням часу (ППЧ) і їх комбінацій [1–4]. Найбільш широке поширення у військових СРЗ отримали сигнали з ППРЧ.

На сьогоднішній день в тактичній ланці управління Збройних сил (ЗС) України широко використовуються радіостанції виробництва компаній "L3 Harris Technologies" (США) та

"Aselsan A.Ş." (Туреччина), побудовані на основі технології програмно-забезпеченого радіо (SDR, software-defined radio).

Відповідно до рекомендацій [5], до радіопристроїв з програмованими параметрами (Cognitive Radio System, CRS) відносяться радіопередавач і / або радіоприймач, який використовує технологію, що дозволяє за допомогою програмного забезпечення встановлювати або змінювати робочі радіочастотні параметри, включаючи, зокрема, діапазон частот, тип модуляції або вихідну потужність, за винятком зміни робочих параметрів, що використовуються в ході звичайної, попередньо визначеної роботи з попередніми установками радіопристрою, згідно з тією чи іншою специфікацією або стандартом системи.

Для забезпечення стійкого завадозахищеного зв'язку в умовах активної радіоелектронної протидії противника в радіостанціях "Harris" та "Aselsan" передбачені режими роботи з ППРЧ.

Вибір конкретного режиму роботи з ППРЧ залежить від виду завад, що впливають на роботу СРЗ. Залежно від зміни характеру діючих завад повинні змінюватися і режими роботи з ППРЧ.

Багатоваріантність режимів роботи з ППРЧ створює проблему вибору оптимального режиму з врахуванням завадової обстановки у каналі зв'язку та необхідності оперативної зміни вибраного режиму при зміні умов прийому у одного чи декількох абонентів. Чим більший набір можливих режимів роботи запрограмовано у радіостанції, тим важче оператору здійснювати необхідне управління (знаходити правильні рішення). Аналогічна проблема може виникати і перед організаторами мереж радіозв'язку.

Правильний (оптимальний) вибір режиму роботи радіостанції з ППРЧ забезпечить підвищення завадозахищеності СРЗ, що в умовах активної радіоелектронної протидії противника набуває особливої актуальності та вимагає постійного вдосконалення засобів радіозв'язку й ефективного використання їх експлуатаційних характеристик на основі досягнень сучасної науки.

Тому постає актуальною задача аналізу завадозахищених режимів роботи сучасних військових УКХ радіостанцій тактичної ланки управління та розробка практичних рекомендації щодо їх використання.

Актуальність викладеного матеріалу полягає в тому, що в умовах постійного вдосконалення форм і методів ведення бойових дій, високого динамізму зміни станів інформаційно-телекомунікаційних систем тактичної ланки управління, які обумовлені характером бойових дій, а також зміни підходів до планування бойового застосування систем радіозв'язку актуальним залишається питання підвищення завадозахищеності ліній радіозв'язку на основі досягнень сучасної науки.

Аналіз останніх публікацій

Метод розширення спектру радіосигналів на основі ППРЧ є достатньо вивченим і відображеним в науковій літературі.

В роботах [1; 2] викладені основні принципи і характеристики методу ППРЧ, проведений аналіз можливих способів підвищення завадозахищеності СРЗ з ППРЧ в умовах організованих завад і власних шумів приймальних пристроїв, аналізуються адаптивні алгоритми ППРЧ, описуються алгоритми виявлення сигналів з ППРЧ з метою їх радіоелектронного придушення.

В монографії [2] розглянуто використання ППРЧ для підвищення завадозахищеності СРЗ в умовах радіоелектронного протиборства, наведена загальна характеристика СРЗ з ППРЧ, окремо описані питання завадозахищеності сигналів з ППРЧ.

Разом з тим, наявність таких робіт не знижує на сьогодні актуальність досліджень напрямків підвищення завадозахищеності СРЗ з ППРЧ.

В останніх публікаціях пропонуються нові та покращені методики оптимізації (ускладнення алгоритму) формування сигналу ППРЧ, виходячи з аналізу можливої завадової обстановки в радіоканалі та характеристик методів ППРЧ.

Так, у роботі [6] запропоновано метод автоматичного визначення тривалості частотних елементів радіосигналу з ППРЧ за умов наявності вузькосмугових завад у частотному діапазоні роботи радіозасобів.

У роботі [7] запропоновано методику вибору необхідної ширини хопсету, при якій забезпечується задана якість передачі інформації.

У роботах [8; 9] розроблені методики формування сигналу ППРЧ при передачі голосу (мови). Сутність методики [8] полягає у роззосередженні у часі сусідніх символів інформаційного сигналу, що потрапляють під вплив завади.

Сутність методики [9] полягає у такому розташуванні символів мовних кадрів на інтервалі частотних елементів сигналу з ППРЧ, при якому завада вражає найменш важливі для відтворення мови символи.

У роботі [10] запропоновано удосконалену методику вибору параметрів багатоантенних систем радіозв'язку з ППРЧ залежно від завадової обстановки.

У роботі [11] запропоновані напрямки підвищення завадозахищеності систем радіозв'язку з ППРЧ та розроблена методика вибору робочих частот з урахуванням стратегій застосування засобів радіоелектронної боротьби (РЕБ) та електромагнітної сумісності (ЕМС) засобів радіозв'язку, що розгортаються в локальних угрупованнях радіозасобів.

У роботі [12] представлений огляд існуючих методів (протоколів) фізичного, канального, мережевого, транспортного та прикладного рівнів передачі даних мереж радіозв'язку, що самоорганізуються, і визначено напрями їх подальших досліджень.

У роботі [13] проведено аналіз завдань, що виникають при розробці та експлуатації СРЗ з ППРЧ, та запропоновано напрямки їх вирішення.

Наукові розробки щодо підвищення завадозахищеності СРЗ з ППРЧ можуть бути використаними при розробці нових вітчизняних радіозасобів або удосконаленні існуючих.

Разом з тим, викладені в зазначених роботах теоретичні основи прогнозування завадової обстановки в радіоканалі, пропозиції щодо покращення алгоритмів формування сигналів з ППРЧ в умовах радіопротидії противника є корисними і для підвищення ефективності використання радіозасобів з ППРЧ, що перебувають на постачанні ЗС України.

Польові посібники оператора (посібники з експлуатації), зокрема остання редакція такого посібника з експлуатації портативної УКХ радіостанції "Harris" RF-7850M-HH [14], не дають рекомендацій щодо вибору режимів роботи з ППРЧ залежно від умов ведення радіозв'язку.

Останні публікації [1–13] щодо завадозахищеності засобів радіозв'язку з ППРЧ дають змогу проаналізувати існуючі режими роботи з ППРЧ, зокрема на прикладі радіостанції "Harris" RF-7850M-HH, і розробити рекомендації щодо їх вибору та налаштування параметрів при плануванні радіомереж тактичної ланки управління.

Мета статті. Метою даного дослідження є проведення аналізу завадозахищених режимів роботи сучасних УКХ радіозасобів військового призначення тактичної ланки управління на прикладі радіостанціїї "Harris" RF-7850M-HH та розробка практичних рекомендацій щодо їх використання.

Виклад основного матеріалу

Коротка характеристика завад

Основними видами завад, які реалізуються в системах РЕБ, є (рис. 1) [1; 2]:

шумова загороджувальна завада;

шумова завада в частині смуги;

полігармонійна завада;

завада у відповідь (ретрансльована завада).

Найбільш універсальною і стійкою до різних способів завадостійкості, що застосовуються в СРЗ, є шумова загороджувальна завада (рис. 1, *а*), моделлю якої є обмежений за смугою адитивний білий гаусівський шум зі спектральною щільністю потужності G_j:

$$G_j = P_j / W_s,$$

де P_j – потужність завади; W_s – смуга частот.

Загороджувальна завада повинна перекривати частотний діапазон СРЗ і при відповідній потужності станції завад здатна придушити СРЗ за будь-яких способів переналаштування частоти. Зважаючи на значний частотний діапазон СРЗ з ППРЧ, потужність передавача завад повинна бути достатньо великою.

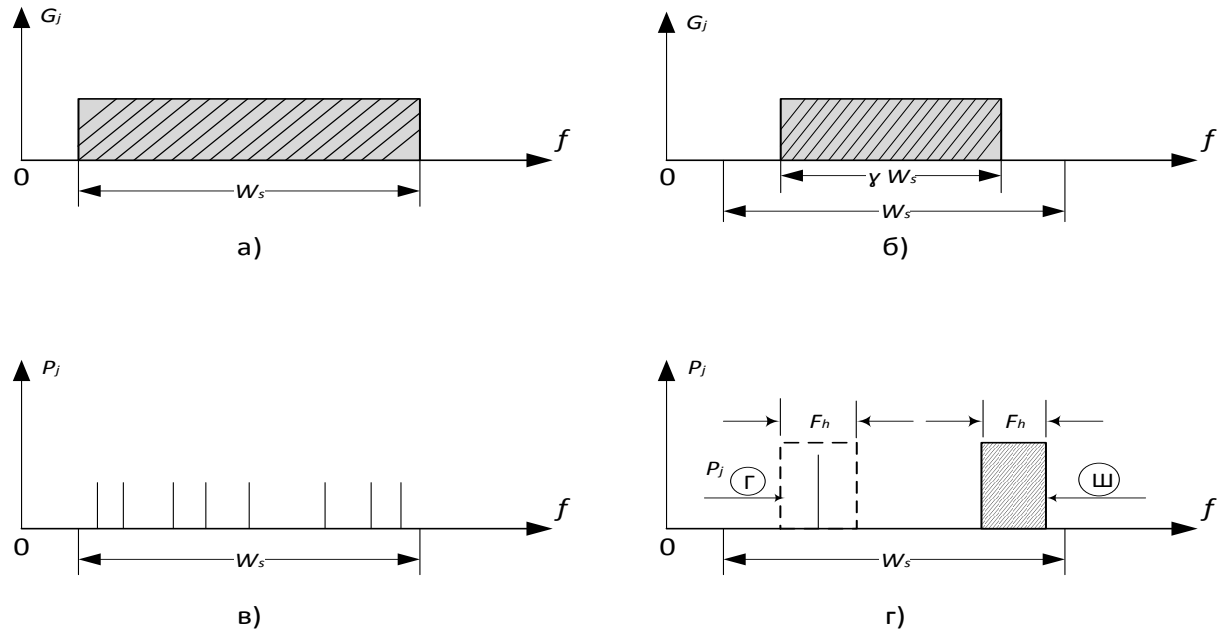

Рис. 1. Основні види завад, що впливають на системи зв'язку з ППРЧ

Потужність шумової завади може бути використана більш ефективно за рахунок зосередження її в обмеженій смузі частот, значно меншій, ніж діапазон частот СРЗ з ППРЧ. Таку заваду прийнято називати шумовою завадою в частині смуги (зосередженою завадою по спектру, завадою з частковим перекриттям спектру сигналів СРЗ) – рисунок 1, *б*.

Спектральна щільність потужності шумової завади в частині смуги G_j може бути представлена у вигляді двох рівнів:

$$G_j = \begin{cases} P_j / (\gamma W_s); в\ смузі (\gamma W_s) \\ 0; W = (1-\gamma) W_s \end{cases},$$

де γ – коефіцієнт, що характеризує частину смуги, яку займає завада, $0 < \gamma < 1$.

Спектральна щільність потужності шумової завади в частині смуги зростає в $1/\gamma$ раз порівняно зі спектральною щільністю потужності шумової загороджувальної завади.

Станція шумових завад з рівномірно розподіленою потужністю в межах смуги γW_s придушує частотні елементи сигналу з ППРЧ з ймовірністю γ. Імовірність того, що ці ж частотні елементи сигналу з ППРЧ не придушуються завадою, дорівнює $(1-\gamma)$.

Для СРЗ з ППРЧ ефективною завадою за певних умов є полігармонійна завада (багатотональна завада), що є набором з l немодульованих гармонійних коливань рівної потужності, розподілених по діапазону частот W_s відповідно до заданої постановником завад стратегії (рис. 1, *в*).

Для створення ефективної полігармонійної завади потрібне досить точне наведення вузькосмугових завад на центральні частоти каналів СРЗ з ППРЧ, а також забезпечення на вході *i*-го каналу приймача СРЗ певного співвідношення потужності завади P_i і потужності сигналу P_s:

$$\frac{P_i}{l} = \frac{P_s}{\alpha},$$

де α – деяке позитивне число (параметр розподілу потужності), яке вибирається постановником завад відповідно до заданої стратегії так, щоб оптимізувати ефективність завади.

При цьому, ефективність гармонійної завади, що діє в тому ж каналі, в якому знаходиться і сигнал, залежить від різниці фаз між завадою і сигналом.

При несприятливих фазових співвідношеннях і рівності $P_j = P_s$ завада може повністю придушити корисний сигнал.

Наявну потужність станції завад найбільш раціонально можна використовувати при створенні завад у відповідь (ретрансльованих завад).

Потужність передавача завад в цьому випадку концентрується лише в смузі частот СРЗ, що придушується, і лише під час її роботи.

У якості завади у відповідь можуть застосовуватися шумова і вузькосмугова (гармонійна) завада (рис. 1, *г*), а також комбінація шумової і вузькосмугової завад.

Завади у відповідь певною мірою є копією частотних елементів сигналу СРЗ, що придушується, і з погляду енергетичних можливостей є одними з найбільш ефективних.

Проте створення завад у відповідь для СРЗ з ППРЧ за порівняно короткий час передачі частотних елементів сигналу (стрибків частоти) наштовхується на технічні й організаційні труднощі.

Серйозною проблемою, з якою стикаються при створенні завад у відповідь, є інтенсивна робота декількох радіоліній з однаковими параметрами налаштувань.

Аналіз завадозахищених режимів роботи УКХ радіостанції "Harris" RF-7850M-HH

Передбачені в радіостанції "Harris" RF-7850M-HH режими роботи з ППРЧ та їх параметри наведені в таблиці 1.

Практичні рекомендації щодо використання режимів роботи з ППРЧ УКХ радіостанції "Harris" RF-7850M-HH в умовах впливу навмисних завад

Загальні підходи до вибору режимів роботи

Радіостанція "Harris" RF-7850M-HH може бути запрограмована для роботи у 25-ти мережах, як у режимі з фіксованою частотою, так і режимах з ППРЧ. 13 мереж можна призначити на відповідні положення поворотного перемикача радіостанції у верхній частині корпуса. Такі можливості радіостанції дозволяють на етапі планування радіомереж передбачати різні варіанти роботи в одних і тих же мережахзалежно від прогнозованої завадової обстановки в каналі зв'язку.

При цьому, необхідно враховувати необхідність:

- ускладнення для противника можливостей по виявленню факту роботи радіостанції в мережі (виявлення сигналу);
- максимальної протидії (за можливості затримки в часі) визначення противником структури виявленого сигналу та його основних параметрів;
- оперативного реагування (зміни режиму роботи) при проявах роботи засобів РЕП противника (при виявленні факту постановки противником навмисних завад);
- забезпечення ЕМС своїх радіоелектронних засобів (РЕЗ).

Зазначені дії є складовою радіоелектронного захисту, який організується і здійснюється для захисту своїх радіоелектронних засобів від радіоелектронної розвідки, вогневого і радіоелектронного впливу противника та від взаємних завад.

Таблиця 1

Режими роботи УКХ радіостанції «Harris» RF-7850M-HH з ППРЧ

№ з/п	Параметр	Quicklook 1A (QL1A)	Quicklook 2 (QL2)	Quicklook 3 (QL3)					Quicklook Wide (QLW)	TNW	
				FCS	Slow	Medium	Fast	Auto		TNW-25	TNW-75
1	**Тип трафіку**	голос, дані	голос						голос, дані		
2	**Синхронізація часу**	не потребують	потребують синхронізації часу TOD (Time-of-day, час дня) вручну (в межах ±1 хв по всій мережі) або за допомогою системи Global Positioning System (GPS)							потребують синхронізації часу TOD вручну (в межах ±1,5 хв) або за допомогою GPS	
3	**Хопсет (Hopset)**	передача та прийом на одному чи на різних хопсетах						передача та прийом на одному хопсеті			
4	**Ширина каналу (Bandwidth)**	25 кГц							75 кГц	25 кГц	75 кГц
5	**Доступ до каналу (Channel Access)**	NONE (ніякого, без організації доступу) або MACA, MACA2	NONE (ніякого, без організації доступу)						MACA2	TNW	
6	**Швидкість стрибків (Hop Rate)**	більше ніж 100 за секунду	більше ніж 300 за секунду	Автома-тичний пошук вільного каналу	більше ніж 100 за секунду	більше ніж 300 за секунду	більше ніж 1000 за секунду	автоматичний вибір підрежимів FCS або ППРЧ зі швидкістю стрибків, вказаною оператором (Slow, Medium, Fast)	більше ніж 100 (або 300) за секунду	більше ніж 100 за секунду	більше ніж 300 за секунду
7	**Вузькосмуговий ключ TRANSEC (NB TRANSEC Key)**	не застосовується	застосовується								

№ з/п	Параметр	Quicklook 1A (QL1A)	Quicklook 2 (QL2)	Quicklook 3 (QL3)				Quicklook Wide (QLW)	TNW	
				FCS	Slow	Medium	Fast	Auto	TNW-25	TNW-75
8	**Криптографічний алгоритм безпеки зв’язку COMSEC Crypto Algoritm)**	Citadel-128, Citadel-256, AES-128, AES-256							AES-256	
9	**Ідентифікатор радіостанції (Radio ID)**	використо-вується, якщо Channel Access – MACA або MACA2	не використовується					використовується		
10	**Ідентифікатор мережі (Network ID)**	не використовується	використовується					використовується		
11	**Модуляція (Modulation)**	Hopping FSK (стрибкоподібна частотна маніпуляція)								
12	**Швидкість передачі (Baud Rate)**	1,6 кбіт/с, 2,7 кбіт/с, 8 кбіт/с, 16 кбіт/с	16 кбіт/с	16 кбіт/с	16 кбіт/с	12 кбіт/с	2,4 кбіт/с	2,4 кбіт/с, 12 кбіт/с, 16 кбіт/с	при 100 стрибках (64 кбіт/с) при 300 стрибках (4,8 кбіт/с, 8 кбіт/с, 24 кбіт/с, 48 кбіт/с)	2,4 кбіт/с	14 кбіт/с на мережу
13	**Вокодер, голосовий режим (Vocoder, Voice Mode)**	MELP, CVSD					MELP	MELP, CVSD		MELP

Загалом, радіоелектронний захист – це комплекс організаційно-технічних заходів і дій, спрямованих на забезпечення стійкої роботи своїх систем управління військами (силами) і зброєю [15].

Організаційні заходи полягають у виборі доцільних способів бойового застосування і розміщення радіоелектронних об’єктів і засобів на місцевості в угрупованнях військ, регламентуванні роботи РЕЗ по території, частотах, режимах і часу, а також у виявленні джерел ненавмисних (взаємних) завад і вжитті заходів щодо виключення їх впливу.

Технічні заходи полягають у застосуванні спеціальних пристроїв, схем захисту і режимів роботи РЕЗ.

Вибір оптимальних режимів роботи радіостанції та параметрів їх налаштування дозволяє підвищити завадозахищеність радіомережі в умовах впливу навмисних завад та зменшити рівень взаємних завад з іншими радіоелектронними засобами та системами.

Оператор радіостанції повинен володіти інформацією щодо запрограмованих режимів роботи тазнати їх основні параметри. Бажано на організаційному рівні завчасно підготувати відповідні пам’ятки операторам радіостанцій, що дозволить в складних умовах бойового застосування приймати відповідні рішення.

На етапі входження в зв’язок необхідно забезпечити обмін інформацією зі всіма радіостанціями мережі, у тому числі з найбільш віддаленими, з забезпеченням вимог щодо якості зв’язку. При цьому, максимальна прихованість СРЗ буде забезпечуватися при роботі з мінімальною потужністю передавача та виборі режиму роботи з ППРЧ з мінімальною швидкістю переналаштування (зі зростанням швидкості ППРЧ дальність зв’язку знижується) та мінімальною швидкістю передачі інформації (зі зростанням швидкості передачі даних якість зв’язку знижується). Вибраний режим роботи з ППРЧ не повинен вимагати додаткових дій щодо синхронізації радіоканалу (початкова синхронізація виконується при першому включенні радіостанцій).

Аналіз можливих на сьогодні варіантів режимів роботи УКХ радіостанції “Harris” RF-7850M-HH з ППРЧ показує (табл. 1), що всі режими роботи забезпечують передачу голосового трафіку і лише окремі – передачу даних. Відповідно, на етапі планування необхідно враховувати прогнозовану інтенсивність та види трафіку, що передаються в радіомережах.

Слід зазначити, що УКХ радіостанція “Harris” RF-7850M-HH відноситься до серії радіостанцій “Falcon III”. Радіостанції серії “Falcon III” переважають за своїми характеристиками радіостанції попередньої серії “Falcon II” (RF-5800), мають додаткові режими роботи. При цьому, забезпечується сумісність зазначених серій радіостанцій, в тому числі і при роботі з ППРЧ.

Зокрема, зустрічна робота УКХ радіостанцій “Harris” серії “Falcon III” (RF-7850V, M) з УКХ радіостанціями “Harris” серії “Falcon II” (RF-5800V, M) з ППРЧ можлива в режимах “Quicklook 1A” та “Quicklook 2”.

На постачанні ЗС України перебувають УКХ радіостанції “Harris” переважно серії “Falcon III”, тому, зважаючи на універсальність режиму роботи з ППРЧ “Quicklook 3”, планування роботи радіостанцій “Harris” RF-7850M-HH в режимі “Quicklook 2” видається недоцільним.

В режимі “Quicklook 1A” забезпечується передача голосового трафіку і даних. За швидкістю ППРЧ (100 стрибків частоти за секунду) режим “Quicklook 1A” відповідає підрежиму “Slow” (низька швидкість) режиму “Quicklook 3”. При цьому, підрежим “Slow” режиму “Quicklook 3” є більш захищеним порівняно з “Quicklook 1A” за рахунок шифрування службового трафіку між радіостанціями в радіомережі (застосовується ключ TRANSEC). Крім того, в режимі “Quicklook 3” оператору з передньої панелі радіостанції доступний вибір підрежимів роботи (Slow, Medium, Fast – низький, середній, швидкий). Синхронізація радіостанцій при роботі в режимі “Quicklook 3” особливих труднощів не викликає і здійснюється або вручну (в межах ±1 хв по всій мережі) або за допомогою системи Global Positioning System (GPS). Відповідно, використання режиму “Quicklook 1A” доцільно розглядати лише для забезпечення передачі даних.

Практичні рекомендації щодо використання режимів роботи з ППРЧ при передачі голосового трафіку

Враховуючи перераховане вище, входження в зв’язок з метою передачі голосового трафіку в умовах впливу навмисних завад пропонується здійснювати у підрежимі “Slow” (низька швидкість, більше ніж 100 стрибків частоти на секунду) режиму “Quicklook 3”. Із можливих величин потужності передавача (Low, Med, High, High+, 1 Вт, 2 Вт, 5 Вт, 10 Вт) спершу вибирається Low, потім Med і т. д. Тобто, забезпечується робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення заданої якості зв’язку.

Для постановника завад закон переналаштування частоти в СРЗ з ППРЧ невідомий. Фундаментальний принцип псевдовипадковості сигналів перешкоджає системі РЕП противника добиватися ефективного впливу організованих завад на СРЗ з ППРЧ. Це змушує систему РЕП з обмеженою потужністю передавача розподіляти відповідним чином спектральну щільність потужності завади по частотному діапазону радіостанції. УКХ радіостанція “Harris” RF-7850M-HH працює в діапазоні частот 30–512 МГц.

На постановку противником шумової загороджувальної завади, або що більш імовірно, зважаючи на зазначене вище, шумової завади в частині смуги і, як наслідок, падіння якості зв’язку нижче порогового рівня, оператору простіше всього відреагувати збільшенням потужності передавача. Однак, збільшення потужності передавача хоч і збільшує завадостійкість, проте є неефективним і неприпустимим з погляду забезпечення прихованості та ЕМС в СРЗ. Роботу передавача з максимальною потужністю можна розглядати як вимушений і тимчасовий режим (протягом нетривалого часу).

Іншим способом, є перехід на інше налаштування режиму “Quicklook 3” (без зміни підрежиму “Slow”), а саме з використанням хопсетів у інших ділянках робочого діапазону частот, а також хопсетів з більшою шириною. При цьому, потрібно мати на увазі, що зі збільшенням ширини хопсету погіршується якість зв’язку [1; 2], що обумовлено наступними основними чинниками:

закони поширення радіохвиль відрізняються для різних частотних елементів, і ця різниця тим більше, чим далі вони рознесені по частотній осі;

чим більша ширина хопсету, тим більше у його межах відрізняються електричні характеристики антени.

Крім цього, більші значення ширини хопсету призводять до зростання ймовірності виникнення взаємних завад з іншими радіоелектронними засобами.

Якщо вибір інших хопсетів в межах режиму “Quicklook 3” не дає бажаного результату, то можливо зробити висновок, що противник застосував заваду у відповідь (ретрансльовану заваду). Ефективний вплив завади у відповідь на СРЗ з ППРЧ може бути досягнутим лише за умови знання постановником завад відповідних параметрів сигналів радіостанції, зокрема, центральних частот каналів, швидкості стрибків частоти, ширини хопсету, потужності сигналу й завади в точці прийому.

Боротися з такою завадою можливо за рахунок збільшення швидкості ППРЧ або шляхом застосування режиму роботи TNW (TDMA Networking Waveform, мережева форма сигналу з множинним розподілом доступу за часом).

Оператор УКХ радіостанції “Harris” RF-7850M-HH може перейти на роботу в підрежимі “Medium” режиму “Quicklook 3” (середня швидкість, 300 стрибків частоти за секунду). Знову ж, за аналогією роботи в підрежимі “Slow” можна випробувати варіанти роботи на різних хопсетах, в тому числі з організацією прийому та передачі інформації на різних хопсетах.

Підрежим “Fast” (швидкий) забезпечує більше ніж 1000 стрибків частоти за секунду. При цьому, завадозахищеність радіостанції максимальна, а дальність зв’язку відповідно мінімальна порівняно з іншими режимами.

Для забезпечення роботи СРЗ в складних умовах завадової обстановки в каналі зв’язку, що постійно змінюється, в УКХ радіостанції “Harris” RF-7850M-HH передбачені адаптивні підрежими роботи “Quicklook 3”:

- режим пошуку вільного каналу (Free Channel Search, FCS);
- змішаний режим (Auto, автоматичний).

Режим пошуку вільного каналу є симбіозом режиму роботи на фіксованій частоті (Fixed Frequency, FF) і ППРЧ. В межах вибраного хопсету здійснюється сканування частотних каналів з метою пошуку вільної (не зайнятої, з найменшим рівнем шумів) частоти. На вибраній фіксованій частоті здійснюється робота, допоки якість зв’язку відповідає встановленим вимогам. У разі зростання рівня шумів понад граничний рівень, радіостанція автоматично переналаштовується на іншу вільну частоту.

Змішаний режим – це ще більш складний адаптивний режим роботи. Залежно від завадової обстановки радіостанція автоматично вибирає, чи використовувати режим пошуку вільного каналу (FCS), чи роботу з ППРЧ зі швидкістю, яку задав оператор (Slow, Medium, Fast).

В умовах завадової обстановки, яка ускладнює передачу інформації в режимі “Quicklook 3”, видається доцільним організувати роботу радіомережі в режимах TNW (“TNW-25”, “TNW-75”).

TNW – розроблений вид сигналу для організації мереж у відносно вузькій смузі частот (25 кГц або 75 кГц). TDMA – це загальний протокол зв’язку, згідно з яким кожна радіостанція, що стає на передачу, отримує доступ до каналу у визначений для неї часовий проміжок. TDMA дозволяє радіостанціям сумісно використовувати один і той же канал передачі, розділяючи сигнали на різні часові інтервали. Мережа TNW використовує форму самоорганізованої децентралізованої мережі та забезпечує контроль як синхронізації часу між радіостанціями, так і розподілу слотів для передачі. Більше того, вона може дуже швидко адаптуватися до змін в топології для гарантування безперервної роботи. Мережа TNW підтримує від 4 до 64 користувачів. TNW використовує ППРЧ з доступом до каналу TDMA і шириною смуги каналу 25 кГц (“TNW-25”) або 75 кГц (“TNW-75”). В режимі “TNW-25” швидкість ППРЧ складає не менше 100 стрибків частоти за секунду, а в режимі “TNW-75” – не менше 300 стрибків частоти за секунду. Для роботи мережі TNW необхідна синхронізація між радіостанціями. TNW автоматично визначає станцію для використання як “ведучої”. Для початку роботи мережі необхідно мати радіостанції з синхронізованим часом, що забезпечується або через GPS, або введенням операторами значення часу з похибкою ±1,5 хв.

Поєднання в мережах TNW методу часового розподілу доступу радіостанції до каналу з алгоритмом ППРЧ є ефективним методом боротьби з радіопротидією противника.

Основними перевагами режиму “TNW-75” над режимом “TNW-25” крім більшої швидкості ППРЧ є:

- повна підтримка IP-протоколу;
- можливість пересилати IP-дані додатковим стрибком (хопом);
- більша пропускна здатність;
- можливість перепризначення слотів для даних.

Практичні рекомендації щодо використання режимів роботи з ППРЧ при передачі даних

Для передавання даних в радіомережах, побудованих на радіостанціях “Harris” RF-7850M-HH, використовуються режими роботи “Quicklook Wide”, “Quicklook 1A” та “TNW-75” (в режимі “TNW-25” забезпечується передача голосового трафіку та даних звітів GPS).

При цьому, якщо за критерій оцінки вибрати швидкість передачі даних, то основним режимом роботи радіостанції “Harris” RF-7850M-HH для передачі даних видається режим роботи “Quicklook Wide”, який потребує широкосмугового радіоканалу (75 кГц).

Найвища заявлена швидкість передачі даних в мережах, побудованих на радіостанціях “Harris” RF-7850M-HH при роботі в режимі “Quicklook Wide”, – до 64 кбіт/с при 100 стрибках частоти за секунду, до 48 кбіт/с при 300 стрибках частоти за секунду. В режимі “Quicklook 1A” швидкість передачі даних до 16 кбіт/с (100 стрибків частоти за секунду). В режимі “TNW-75” (300 стрибків частоти за секунду) IP-дані передаються радіоканалом з максимальною сумарною швидкістю до 14 кбіт/с в межах мережі. Кожному користувачеві визначається швидкість передачі даних на основі кількості запрограмованих учасників мережі. Тобто, сумарна швидкість розподіляється рівномірно за кількістю учасників мережі. Для прикладу, при 10

учасниках мережі TNW для кожної окремої станції виділяється слот з ресурсом швидкості до 1,4 кбіт/с. Якщо ж з’являються додаткові слоти, вони можуть бути перепризначені певним користувачам для додаткових можливостей передачі даних. Для прикладу, мережа запрограмована для роботи 10 учасників, реально працюють 6 учасників. В такому випадку 4 слоти для передачі можуть бути перепризначені для реально працюючих користувачів.

Таким чином, при організації радіомереж з приорітетною передачею даних по відношенню до голосового трафіку доцільним видається використання режиму “Quicklook Wide”.

Висновки

Спираючись на проведений в матеріалах дослідження аналіз, стає можливим зробити наступні висновки:

1) забезпечення стійкого радіозв’язку в умовах складної радіоелектронної обстановки, яка постійно змінюється, можливо за рахунок вибору режимів роботи СРЗ із заздалегідь налаштованими параметрами;

2) рішення щодо вибору режимів роботи в радіолінії повинні прийматися на основі аналізу стану каналу зв’язку;

3) в умовах застосування противником засобів радіоелектронного придушення, режими роботи радіостанцій повинні узгоджуватися з видами завад і мінімізувати помилки сигналів, що приймаються;

4) вибір оптимальних режимів роботи в радіолінії напряму залежить від можливостей, в тому числі і технічних, щодо ідентифікації завадової обстановки в каналі зв’язку. Критично важлива інформаційна взаємодія з підрозділами радіоелектронної розвідки з метою отримання відомостей щодо засобів РЕБ противника та характеру випромінюваних ними сигналів;

5) у випадку відсутності впливу навмисних і випадкових завад, крім шумового фону, необхідність роботи в режимах з ППРЧ відпадає. Більш того, невиправдане включення цих режимів погіршує якість радіозв’язку через додаткові втрати і затримки при складних перетвореннях сигналів;

6) прийняття оператором оптимальних рішень щодо вибору завадозахищених режимів роботи СРЗ можна досягнути шляхом автоматизації процесу моніторингу стану каналу зв’язку і підготовки пропозицій щодо режимів роботи радіостанції залежно від завадової обстановки. Це можливо за рахунок удосконалення як апаратної частини радіостанцій так і програмного забезпечення.

Програмне забезпечення УКХ радіостанцій “Harris” RF-7850M-HH постачається виробником, компанією “L3 Harris Technologies” (США). Можливо допустити, що в наступних версіях мікропрограм (актуальна версія 4.7.0) можуть з’явитися додаткові опції [16], в тому числі і щодо автоматизації вибору запрограмованих режимів роботи залежно від стану каналу зв’язку (змішаний режим “Quicklook 3” тому свідчення).

Напрямом перспективних досліджень є:

1) дослідження в галузі розробки окремого дистанційного пристрою з відповідним програмним забезпеченням, який буде підключатися до радіостанції (через боковий роз’єм) і забезпечувати автоматичну ідентифікацію завадової обстановки і автоматичний (або автоматизований, на рівні видачі варіантів для прийняття рішення) вибір оптимального режиму роботи радіостанції;

2) впровадження технологій когнітивного радіо (CR, Cognitive Radio), які дозволять автоматично проводити аналіз завадової обстановки і відповідний вибір частотного піддіапазону, підстроювання частотних, часових й енергетичних параметрів, режимів роботи та форм сигналів радіостанцій, що налаштовуються програмно;

3) проведення натурних випробувань із залученням сучасних засобів РЕБ для визначення ефективності (завадозахищеності) роботи радіомереж у різних режимах та розробка інструкцій щодо забезпечення функціонування СРЗ в умовах впливу радіозавад.

ЛІТЕРАТУРА

1. Борисов В. И., Зинчук В. М., Лимарев А. Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты: под ред. В. И. Борисова. Изд. 2-е, перераб. и доп. Москва: Радио Софт, 2008. 512 с.

2. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография. Санкт-Петербург: Свое издательство, 2013. 166 с.

3. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва: Радио и связь, 1985. 384 с.

4. Помехозащищенность радиосистем со сложными сигналами / Тузов Г. И. и др.; под ред. Г. И. Тузова. Москва: Радио и связь, 1985. 264 с.

5. Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS): отчет МСЭ-Р SM.2152: вебсайт. URL: https://www.itu.int/pub/R-REP-SM.2152-2009 (дата звернення 24.03.2022).

6. Нагорнюк О. А. Метод автоматичного визначення часових параметрів радіосигналів із псевдовипадковим перестроюванням робочої частоти на фоні вузькосмугових перешкод. *Збірник наукових праць ЖВІ.* 2018. Вип. 15. С. 53–64.

7. Кривенко О. В. Методика формування сигналу в радіозасобах з ППРЧ в умовах впливу навмисних шумових завад. *Системи озброєння і військова техніка.* 2017. № 1 (49). С. 132–135.

8. Гурський Т. Г. Підвищення завадозахищеності радіоліній з ППРЧ в умовах завад у відповідь. *Збірник наукових праць Харківського університету Повітряних Сил.* 2014. Вип. 3 (40). С. 58–63.

9. Гурський Т. Г., Кривенко О. В. Методика формування сигналу в радіозасобах з ППРЧ при передачі мови в умовах впливу завад у відповідь. *Системи управління, навігації та зв’язку.* 2017. Вип. 2 (42). С. 179–184.

10. Шишацький А. В., Кувшинов О. В., Петрунчак С. П. Методика вибору раціональних значень параметрів багатоантенних систем військового радіозв’язку з псевдовипадковою перестройкою робочої частоти. *Системи озброєння і військова техніка.* 2017. № 2 (50). С. 151–155.

11. Кувшинов О. В., Шишацький А. В., Жук О. Г., Бєляков Р. О., Прокопенко Є. М., Леонтьєв О. Б., Животовський Р. М., Дробаха Г. А., Романенко І. О., Петрук С. М. Розробка методики підвищення завадозахищеності засобів радіозв’язку з псевдовипадковою перестройкою робочої частоти. *Східно-Європейський журнал передових технологій.* 2019. Том 2, № 9 (98): Інформаційно-керуючі системи. С. 74–84.

12. Романюк В. А., Степаненко Є. О., Панченко І. В., Восколович О. І. Літаючі самоорганізуючі радіомережі. *Збірник наукових праць ВІТІ.* 2017. Вип. 1. С. 104–114.

13. Гурський Т. Г., Жук О. Г., Кривенко О. В., Шишацький А. В. Напрямки вдосконалення засобів радіозв’язку з псевдовипадковою перестройкою робочої частоти. *Збірник наукових праць ВІТІ.* 2016. Вип. 1. С. 25–34.

14. RF-7850M-HH. Багатодіапазонна портативна радіостанція: посібник з експлуатації: ТОВ “Радіо Сатком Груп”, 03067, м. Київ, вул. Машинобудівна, 37, оф. 115. 210 с., перекладено українською мовою з видання Harris Corporation Communication Systems, 1680 University Avenue Rochester, New York 14610-1887 USA Publication Number: 10515-0461-4204 June 2018 Rev. H.

15. ВСТ 01.004.007-2017 (1) Воєнна політика, безпека та стратегічне планування. Система стратегічних комунікацій держави у воєнній сфері. Терміни та визначення: вебсайт. URL: http://stratcom.nuou.org.ua (дата звернення: 07.06.2022).

16. Калашніков І. А. Актуальність оновлення программного забезпечення радіостанцій L3 HARRIS / Збірник матеріалів XIII науково-практичної конференції ВІТІ. Київ, 2020. С. 140.

АВТОРИ НОМЕРА

1. ***Андреєв Андрій Олександрович*** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

2. ***Артемчук Михайло Васильович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

3. ***Бєляков Роберт Олегович*** – кандидат технічних наук, доцент, старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

4. ***Бондаренко Леонід Олександрович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

5. ***Гриценок Костянтин Миколайович*** – начальник кафедри технічного та метрологічного забезпечення факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

6. ***Гулій Володимир Станіславович*** – заступник начальника кафедри технічного та метрологічного забезпечення факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

7. ***Дегтярьов Анатолій Сергійович*** – провідний науковий співробітник науково-дослідного відділу Наукового методичного центру кадрової політики Міністерства оборони України.

8. ***Драглюк Олексій Вікторович*** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

9. ***Залужний Олексій Вікторович*** – кандидат технічних наук, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

10. ***Зінченко Михайло Олександрович*** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

11. ***Кіка Іван Анатолійович*** – співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

12. ***Коротков Михайло Михайлович*** – провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

13. ***Кубік Сергій Іванович*** – науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

14. ***Кузенков Володимир Сергійович*** – співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

15. ***Кузьменко Максим Дмитрович*** – кандидат психологічних наук, начальник науково-дослідного відділу Наукового методичного центру кадрової політики Міністерства оборони України.

16. ***Ляшенко Віктор Олександрович*** – військова частини 0515.

17. ***Любарський Сергій Володимирович*** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

18. **Ольшанский Валентин Вікторович** – доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

19. ***Остапчук Віктор Миколайович*** – начальник Військового інституту телекомунікацій інформатизації імені Героїв Крут, м. Київ, Україна.

20. ***Павлюк Дмитро Олександрович*** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

21. ***Панченко Ігор В’ячеславович*** – кандидат технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

22. ***Плугова Ольга Богданівна*** – науковий співробітник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

23. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, заступник з наукової роботи начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. ***Радченко Микола Миколайович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

25. ***Руденко Володимир Іванович*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

26. ***Слотвінська Людмила Іванівна*** – кандидат технічних наук, доцент, викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

27. ***Філіпов Вячеслав Васильович*** – доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

28. ***Цатурян Олександр Георгійович*** – провідний науковий співробітник проєктно-конструкторського науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

29. ***Цимбал Ірина Володимирівна*** – науковий співробітник проєктно-конструкторського науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

30. ***Чевардін Владислав Євгенійович*** – доктор технічних наук, начальник кафедри, Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

31. ***Ченченко Віктор Анатолійович*** – науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Рукопис статті потрібно подавати разом із зазначеними нижче документами українською мовою:

– *актом експертизи* (1 примірник);

– *рецензіями (зовнішньою або внутрішньою)* – за підписом провідного ученого, який працює в даному напряму досліджень;

– *довідкою про автора (авторів)*.

Рукопис подається у двох видах: на флеш-пам'яті або CD, розпечатаний на лазерному принтері (1 примірник), у текстовому редакторі – **Microsoft Word 10**, а також може бути надісланий за електронною адресою: **naukaviti@gmail.com.**

Формат аркуша – **А4 (210 мм × 297 мм)**.

Розмір полів: зліва – **20 мм**, справа – **20 мм**, зверху – **20 мм**, знизу – **20 мм**.

Стиль – **normal** (звичайний), інтервал між рядками – **1,0**, абзацний відступ – **1 см**. Шрифт – **Times New Roman № 12**, із виключенням переносів.

Анотацію друкують курсивом, шрифт **Times New Roman № 10.** Анотацію та ключові слова приводять українською та англійською мовами. Обсяг кожної з них не менше 1800 знаків з побілами, включаючи ключові слова. Анотація повинна бути структурована таким чином: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації ключові слова українською, англійською мовами. Список використаних джерел оформляється 11 шрифтом, згідно з ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання (не використовувати тире «–»).

Етапи представлення статті для науковців інституту:

1. Стаття подається на розгляд головному редактору та після погодження – відповідальному редактору.

2. Після позитивного розгляду редколегією стаття подається коректору (кімната № 5 редакційно-видавничого відділу) для вичитки та корегування.

Виправлення електронного варіанта статті.

Друкування виправленого варіанта статті, отримання розпису коректора про виправлення помилок, що були виявлені, на останньому аркуші статті.

3. Виправлена стаття передається разом із супровідними документами відповідальному редактору для формування комп'ютерного макета збірника.

Не зараховуються праці, у яких відсутній повний опис наукових результатів, що засвідчує їх, достовірність, або в яких повторюються результати, опубліковані раніше в інших наукових працях, що входять до списку основних (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Статті, які містять загальновідому науково-технічну інформацію, плагіат, не розглядаються й не друкуються.

В один випуск «Системи і технології зв'язку, інформатизації та кібербезпеки» приймається не більше однієї статті за темою дисертації (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Тексти статей та їхні копії на магнітних чи оптичних носіях авторам не повертаються.

Редакційна колегія залишає за собою право вносити зміни в рукопис редакційного характеру.

Телефон для довідок: 256-22-37, 256-22-73, внутрішній 442-37, 442-73.

Електронна адреса для надання статей: naukaviti@gmail.com, naukaviti@viti.edu.ua.