УДК 621.391.8:004.89:004.056.5 **DOI:10.30837/rt.2025.4.223.14**

L.I. MELNIKOVA, Ph.D. (Tech. Sci.), O.V. LINNYK, Ph.D. (Tech. Sci.),
S.V. SHTANGEI, Ph.D. (Tech. Sci.)

HIERARCHICAL CLUSTERING USING A KOHONEN NEURAL NETWORK FOR SECURED WIRELESS SENSOR NETWORKS

Introduction

In today's world, wireless sensor networks (WSNs) have found wide application in environmental monitoring systems, smart cities, healthcare, and military technologies [1-6]. Despite their flexibility and scalability, WSNs remain vulnerable to a broad spectrum of cyber threats from data interception to routing manipulation and node spoofing [1].

Current research treats WSN security as a multidimensional problem encompassing power consumption, data processing, and protection against both internal and external threats [1]. A WSN consists of a large number of sensor nodes with severe resource constraints, which complicates the use of classical cryptographic techniques.

Because the topology of a WSN can change through node failure, the deployment of new sensors, or node mobility protection methods must adapt to these changes in real time. Classical encryption delivers a high level of confidentiality but is often too resource hungry for battery powered nodes. Consequently, there is a need for intelligent clustering systems that can dynamically reconfigure cluster boundaries, classify nodes by behavioral characteristics,) integrate new nodes without compromising network integrity, and respond promptly to security threats [1, 7, 8].

Network robustness is a primary quality of service metric for WSNs because sensor nodes are frequently deployed in locations where direct maintenance battery replacement or repair is infeasible. Quantitatively, robustness can be expressed as the time required to restore normal operation after a topology change. This property is determined mainly by the organization of routing and by the way individual nodes acquire information about their neighbors (routing tables, periodic neighbor advertisements).

Clustering is the most important structural technique for prolonging the lifetime of a WSN and reducing its energy consumption. It also supports periodic rotation of the cluster head role, thereby balancing the load among nodes over the network's life cycle [9].

One promising direction for strengthening WSN security is to employ machine learning methods for anomaly detection and node classification. In particular, the Kohonen neural network or self organizing map (SOM) has shown great potential in clustering, intrusion detection, and adaptive data processing.

This paper proposes an innovative approach to information security in WSNs based on node clustering with a Kohonen network.

Survey of Clustering Algorithms in WSNs and Problem Statement

Clustering (or cluster analysis) is the task of partitioning a set of objects into groups clusters. Objects within the same cluster should be similar, whereas objects belonging to different clusters ought to exhibit the greatest possible dissimilarity. A wireless sensor network (WSN) comprises a multitude of sensor nodes capable of sensing the state and parameters of the physical world, storing and processing this information, and transmitting it over communication channels. In WSNs, clustering algorithms address node self-organization, minimize energy consumption, extend overall network lifetime, perform data aggregation, accelerate data transmission and processing, and enlarge the network's coverage area.

Two principal architectural paradigms exist for sensor networks: homogeneous and hierarchical (cluster-based). In a homogeneous architecture every node performs identical functions. The

alternative is hierarchical (tree-like) routing, which partitions the network into clusters. Each cluster is governed by a cluster head that aggregates information from the other nodes and forwards it to a gateway. The cluster-head role is periodically rotated to equalize the energy expenditure among all sensor nodes. An appropriate choice of network architecture markedly increases WSN efficiency.

In the cluster-formation algorithm proposed by the authors of [9], Voronoi diagrams are employed. During each round the sensor field is randomly partitioned. After a cluster head has been selected, the distance between every sensor node and that head is computed. The algorithm relies on two parameters for cluster-head election in a WSN: residual energy and Voronoi-based centrality. Both quantities are evaluated using fuzzy-logic methods. Hierarchical clustering with low power consumption is likewise realized in WSNs via the Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm [10]. The network life-cycle consists of a cluster-formation phase followed by transmission of the aggregated data to the gateway.

The Fuzzy C-Means (FCM) algorithm likewise consists of cluster-formation and cluster-head selection phases in a wireless sensor network. In this approach, FCM is first applied to partition the nodes into clusters; a fuzzy-logic system based on two parameters residual energy and centrality then elects the cluster head. Afterward, data are forwarded hop-by-hop from one cluster head to the next until they reach the base station [11]. The network lifetime is defined as the time interval until the final sensor node ceases to operate. Simulation results show that the algorithm successfully delineates clusters of varying size and selects an appropriate head for each cluster. Hence, the method provides an effective means of organizing a network of dynamically changing nodes.

Research further indicates that clustering not only optimizes data processing and energy consumption but can also enhance network security through localized monitoring, in cluster data filtering, and intrusion detection. Nevertheless, most existing solutions fail to deliver adequate adaptability under conditions of rapid topological change. Despite their methodological variety, the majority of algorithms concentrate on reducing energy usage while neglecting the complex dynamics that characterize modern WSNs.

In a dynamic WSN environment, where sensor nodes may fail or be deployed in real time, an adaptive clustering system is required one that not only optimizes routing but also responds to information-security threats. Classical cryptographic techniques are typically too resource-hungry for sensor nodes, and many clustering algorithms cannot admit new nodes without disrupting existing network logic. Security mechanisms are often restricted to packet-level control, neglecting behavioral anomalies at the node level.

Against this backdrop, clustering based on a Kohonen neural network becomes highly relevant because it can

- classify nodes according to their behavioral patterns,
- form adaptive clusters that track topological changes,
- deliver a rapid response to potential threats.

Unlike the clustering algorithms surveyed in the literature, the proposed Kohonen-based WSN clustering method not only determines cluster centroids but also integrates newly added nodes seamlessly. Kohonen Self-Organizing Maps (SOMs) have proven to be an effective tool for unsupervised clustering, requiring no pre-labelled data an essential advantage when monitoring large-scale WSN deployments where data reliability may fluctuate.

Despite the rapid evolution of data-analysis techniques and security frameworks, adapting them to the operational constraints of WSNs remains an open challenge. Classical encryption is prohibitively expensive for sensor hardware, and naïve node classification schemes do not offer adequate protection against dynamic cyber-threats. Consequently, there is a pressing need for an efficient, adaptive, and resource-conserving approach to information security in WSNs. Self-organizing neural networks especially the Kohonen model enable optimal behavior-based node classification and situational awareness, opening new avenues for early threat detection and the mitigation of their impact.

A Kohonen network is a two-layer neural architecture comprising an input layer and a Kohonen (competitive) layer. The Kohonen layer may be one-, two-, or three-dimensional [12]:

1-D configuration: the competitive neurons are arranged in a linear chain.

2-D configuration: the neurons form a rectangular grid (typically square or rectangular).

3-D configuration: the neurons constitute a lattice in three-dimensional space.

Because no labelled training set is available i.e. there is no teacher specifying the cluster membership of every pattern the weight vectors of the Kohonen layer are learned by classical unsupervised-classification methods (clustering/self-organization) [13,14]. Figure 1 presents a representative topological map of a Kohonen network.

Neurons of the input layer supply the feature values of the patterns to be recognized, whereas the competitive neurons in the Kohonen layer delineate regions (clusters) corresponding to different pattern classes. Each neuron in the Kohonen layer is also connected to its adjacent neurons, forming a neighborhood structure.

Let us introduce the following notation:

$$\vec{W} = \left(w_{j1}, w_{j2}, \ldots, w_{jn}\right)^T, \tag{1}$$

the weight vector of the *j*-th neuron in the Kohonen layer, and

$$\vec{X} = (x_1, x_2, \ldots, x_n)^T, \tag{2}$$

the input (feature) vector of a particular sample.

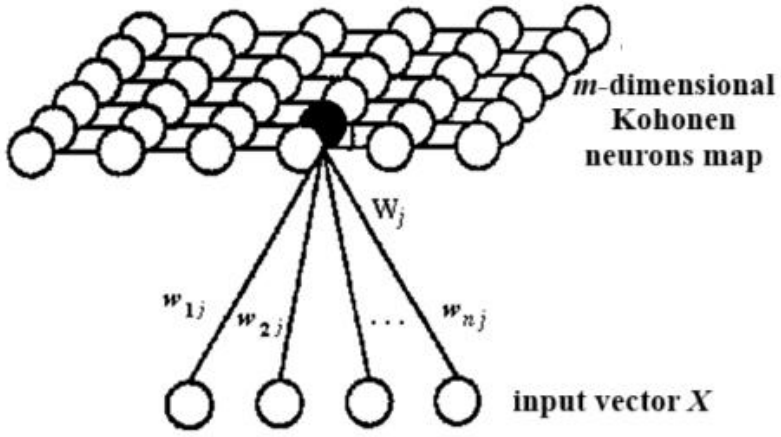

Fig. 1. Example of a topological map of a Kohonen network

During the training (more precisely, self-training) phase, the input vector *X* is compared pairwise with every weight vector *Wj* of the neurons in the Kohonen layer. A proximity (similarity) measure (typically the Euclidean distance) is introduced. The neuron *c* for which the distance *d (X, Wc)* is minimal (or, equivalently, whose similarity is maximal) is declared the winner. The pattern represented by *X* is consequently assigned to the class represented by this winning neuron. In effect, the *n*-dimensional input space *Rn* is mapped onto an *m*-dimensional lattice – the Kohonen layer.

This mapping arises through a recurrent, iterative unsupervised-learning procedure, the hallmark of which is the emergence of clusters. Once self-training is complete, previously unseen input patterns are, in the network's operational phase, assigned to one of the clusters uncovered during training [15].

Simulation of Clustering in WSNs

Modeling was carried out in the Matlab environment; the software implementation is deposited in Zenodo [16]. Random sensor deployment was simulated by generating x,y,z coordinates drawn from a normal distribution. Figure 2 shows the empirical density histogram for sensor coordinates along the *x*-axis: χ^2=12.7933, $P(\chi^2>\chi^2_\alpha)$=0.8000, significance level α=0.05. The null hypothesis of normality for the x-coordinate distribution cannot be rejected at the 5 % level.

Figure 3 presents the corresponding histogram for the *y*-axis: χ^2=17.1648, $P(\chi^2>\chi^2_\alpha)$=0.5000, α=0.05. The null hypothesis of normality for the *y*-coordinate distribution is likewise not rejected.

Figure 4 shows the histogram for the *z*-axis: χ^2=21.5069, $P(\chi^2>\chi^2_\alpha)$=0.2000, α=0.05. Again, the hypothesis of normality for the *z*-coordinate distribution is not rejected by the empirical data.

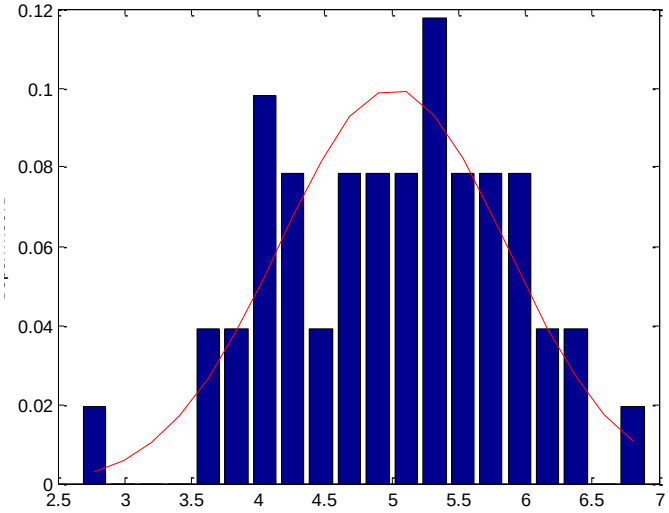

Fig. 2. Density histogram of sensor coordinate distribution along the *x*-axis

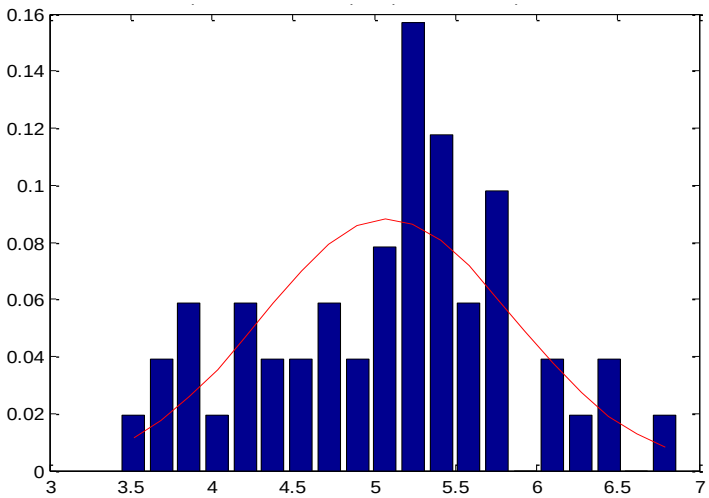

Fig. 3. Density histogram of sensor coordinate distribution along the *y*-axis

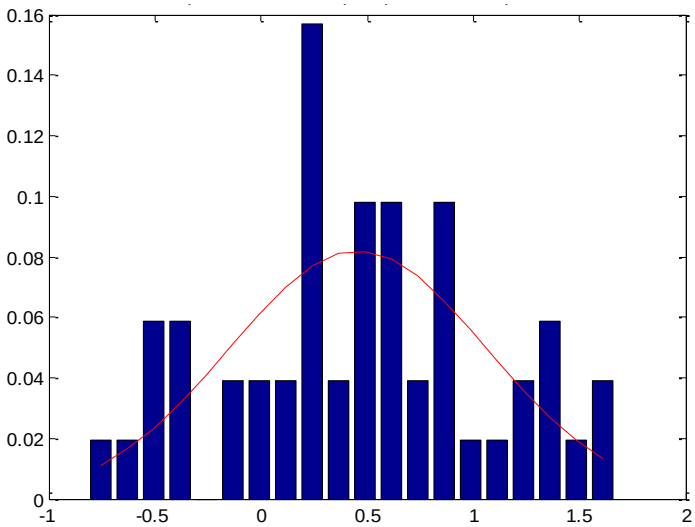

Fig. 4. Density histogram of sensor coordinate distribution along the *z*-axis

Table 1

Pairwise Euclidean distances between the first six sensors of Cluster 1

Sensor №	1	2	3	4	5	6
1	0.0000	1.0622	0.9279	0.9958	1.1649	0.9923
2	1.0622	0.0000	1.8247	1.9231	1.5138	0.9568
3	0.9279	1.8247	0.0000	0.4198	1.5776	1.9019
4	0.9958	1.9231	0.4198	0.0000	1.3149	1.8639
5	1.1649	1.5138	1.5776	1.3149	0.0000	1.2233
6	0.9923	0.9568	1.9019	1.8639	1.2233	0.0000

Three clusters containing 51, 11, and 11 sensors, respectively, were analysed. Figures 5 and 6 depict the spatial and planar positions of sensors across all clusters.

Using a Kohonen network, cluster centroids were identified; these are indicated in Figures 5–6. A newly introduced sensor with coordinates [8; 6; 0.6] was correctly assigned to Cluster 1 (Fig. 7).

Unlike algorithms discussed in the literature, the proposed method not only determines cluster centroids but also seamlessly incorporates new elements into the network. The mapping results from repeated unsupervised learning iterations, culminating in groups of similar elements. Once training is complete, the network can place unseen data into the appropriate pre formed cluster.

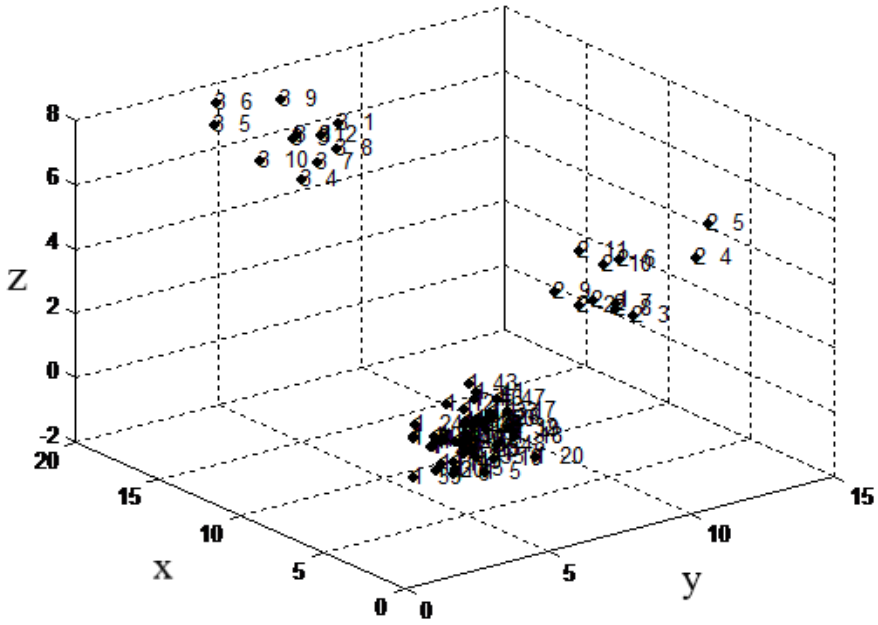

Fig. 5. Spatial distribution of all clusters.

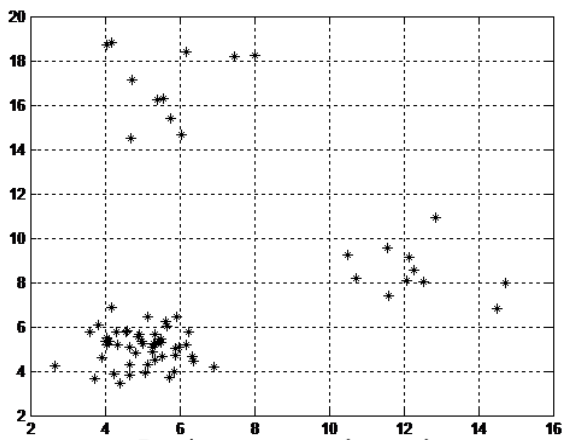

Fig. 6. Planar (2 D) distribution of all clusters

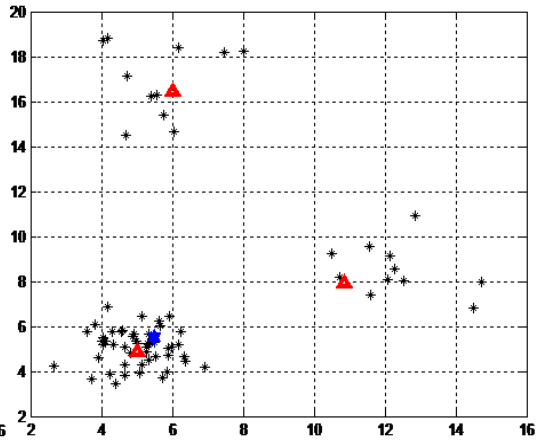

Fig. 7. Integration of a new sensor node

Discussion

Network robustness is a critical quality of service parameter for WSNs operating under dynamic topology changes such as node failure, addition, or relocation. Our simulations show that Kohonen based clustering satisfies this requirement. The proposed approach yields an efficient, flexible, and adaptive WSN structure – especially under dynamic conditions.

Automatic cluster assignment of newly introduced sensors enables rapid adjustment without centralised processing. The self organising nature of the Kohonen map makes it a promising tool for early detection of cyber‑ threats via behavioural classification.

Compared with LEACH and Fuzzy C Means, the neural approach demonstrates superior adaptability under changing topologies and unstable environments.

Conclusions

The conducted simulations of WSN clustering with a Kohonen neural network confirm the effectiveness of adaptive topology management. Generated topological maps illustrate the network's ability to self organise, form stable clusters, and integrate new sensors without disrupting classification logic.

By accounting for residual energy and spatial centrality, the proposed method conserves energy and extends network lifetime. Kohonen clustering not only optimises operation but also acts as an active defence mechanism: localised monitoring, behavioural anomaly detection, and rapid structural adaptation jointly enhance cybersecurity without heavy cryptographic overhead.

References:

1. Ram G.M., IlavarasanE. Security Challenges in Wireless Sensor Network: Current Status and Future Trends // Wireless Pers Commun. 2024. No 139. P. 1173–1202. doi: 10.1007/s11277-024-11660-9

2. Shah SL. Abbas ZH., Abbas G., Muhammad F., Hussien A., Baker T. An Innovative Clustering Hierarchical Protocol for Data Collection from Remote Wireless Sensor Networks Based Internet of Things Applications // Sensors (Basel). 2023 Jun 19;23(12):5728. doi: 10.3390/s23125728.

3. Liu Z, Zhang J., Liu Y., Feng F., Liu Y. Data aggregation algorithm for wireless sensor networks with different initial energy of nodes // PeerJ Comput Sci. 2024 Mar 15;10: e1932. doi: 10.7717/peerj-cs.1932.

4. Melnikova L., Linnyk E., Kryvoshapka M., and Barsuk V. Application of heuristic procedure for multi-criteria optimization to select optimal version of IP network speech codec // Problemi telekomunìkacìj. 2020. No. 1(26). P. 23–32. doi: 10.30837/pt.2020.1.02.

5. Chekubasheva V., Glukhov O., Kravchuk O., Levchenko Y., Linnyk E., Rohovets V. (2022). Possibility of Creating a Low-Cost Robot Assistant for Use in General Medical Institutions During the COVID-19 Pandemic // Blaschke, D., Firsov, D., Papoyan, A., Sarkisyan, H.A. (eds) Optics and Its Applications. Springer Proceedings in Physics. 2022. Vol 281. Springer, Cham. https://doi.org/10.1007/978-3-031-11287-4_16

6. Srinivasan D., Kiran A., Parameswari S., Vellaichamy J. Energy efficient hierarchical clustering based dynamic data fusion algorithm for wireless sensor networks in smart agriculture // Sci Rep. 2025 Feb 28;15(1):7207. doi: 10.1038/s41598-024-85076-7

7. Wang M. and Zeng J. Hierarchical Clustering Nodes Collaborative Scheduling in Wireless Sensor Network // IEEE Sensors Journal. 2022. Vol. 22, no. 2. P. 1786-1798, 15 Jan.15. doi: 10.1109/JSEN.2021.3132504

8. Melnikova L., Linnyk Y., Kryvoshapka M., and Barsuk V. Optimization of mobile drain route in a wireless sensor network // Problemi telekomunìkacìj. 2019. Vol. 0, no. 1(24). P. 104–112, Nov. 2019. doi: 10.30837/pt.2019.1.07.

9. Heinzelman W. B., Chandrakasan A. P., and Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks // IEEE Transactions on Wireless Communications. 2002. Vol. 1, no. 4. P. 660–670. doi: 10.1109/twc.2002.804190.

10. Fuzzy logic-based energy balance routing algorithm in wireless sensor networks // Journal of Xidian University 2020. Vol. 14, no. 12. doi: 10.37896/jxu14.12/017.

11. Firoiu V., Le Boudec J.-Y., Towsley D., and Zhang Zhi-Li. Theories and models for Internet quality of service // Proceedings of the IEEE. Vol. 90, no. 9. P. 1565–1591. doi: 10.1109/jproc.2002.802002.

12. Kohonen self-organising networks, Neural Computing: An Introduction. doi: 10.1887/0852742622/b335c5.

13. Wang Z., Ye M., Cheng J., Zhu C., Wang Y. An Anomaly Node Detection Method for Wireless Sensor Networks Based on Deep Metric Learning with Fusion of Spatial-Temporal Features // Sensors (Basel). 2025. Vol. 25(10). P. 3033. doi:10.3390/s25103033

14. Lv A., Li C., Xie J. and Zhang Z. Research on Routing Algorithm for WSN Based on Hierarchical Clustering // 2021 6th International Conference on Communication, Image and Signal Processing (CCISP), Chengdu, China, 2021. P. 384–388. doi: 10.1109/CCISP52774.2021.9639354.

15. Gatte O. El, A. Abbassi El, Mouhib O., Tilioua A. Performance comparison of different algorithms to secure the information for Wireless sensor Network // ITM Web Conf. 69 04005 (2024). doi:10.1051/itmconf/20246904005

16. Melnikova L. Hierarchical clusterization for securecommunication in sensor networks with Kohonen neural network // Zenodo, Jul. 22, 2025. doi: 10.5281/zenodo.16328467. Available: https://zenodo.org/records/16328467.

17. Raghupathy M., and Chukka Rajasekhar. Deriving a Multi-Objective Function Using Hybrid Meta-Heuristic Approach for Optimal CH Selection and Optimal Routing in WSN // Cybernetics and Systems. 2025, March, 1–42. doi:10.1080/01969722.2025.2468191.

Received 27.09.2025

Information about the authors:

Lyubov Melnikova – Ph.D. (Technical Sciences), Associate Professor, Department of Infocommunication Engineering V.V. Popovsky, Kharkiv National University of Radio Electronics, Ukraine; e-mail: liubov.melnikova@nure.ua; ORCID: https://orcid.org/0000‑0003‑0439‑7108

Olena Linnyk – Ph.D. (Technical Sciences), Associate Professor, Department of Physical Foundations of Electronic Engineering, Kharkiv National University of Radio Electronics, Ukraine; e‑mail: elena.linnyk@nure.ua; ORCID: https://orcid.org/0000‑0002‑4906‑3796

Svitlana Shtangei – Ph.D. (Technical Sciences), Associate Professor, Department of Infocommunication Engineering V.V. Popovsky, Kharkiv National University of Radio Electronics, Ukraine; e‑mail: svitlana.shtanhei@nure.ua ORCID: https://orcid.org/0000‑0002‑9200‑3959.