Харківський національний
університет радіоелектроніки

Kharkiv National
University of Radio Electronics

Державне підприємство
"Південний державний
проектно-конструкторський
та науково-дослідний інститут
авіаційної промисловості"

State Enterprise
"Southern National Design
&
Research Institute
of Aerospace Industries"

СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ

INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES

№ 2 (20), 2022

No. 2 (20), 2022

Щоквартальний науковий журнал

Quarterly scientific journal

Харків
2022

Kharkiv
2022

INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES

No. 2 (20), 2022

АДРЕСА РЕДАКЦІЇ:
Україна, 61166, м. Харків, проспект Науки, 14
Інформаційний сайт: http://itssi-journal.com
E-mail редколегії: journal.itssi@gmail.com

EDITORIAL OFFICE ADDRESS:
Ukraine, 61166, Kharkiv, Nauka Ave, 14
Information site: http://itssi-journal.com
E-mail of the editorial board: journal.itssi@gmail.com

Журнал включено до "Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук" наказом Міністерства освіти і науки України від 16.07.2018 №775 (додаток 7).

Затверджений до друку Науково-технічною Радою Харківського національного університету радіоелектроніки (Протокол № 2 від 30 березня 2022 р.).
Свідоцтво про державну реєстрацію журналу Серія КВ № 22696-12596Р від 04.05.2017 р.

СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ

№ 2 (20), 2022

ЗМІСТ

Інформаційні технології

Сучасні технології управління підприємством

Інженерія та промислові технології

INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES

No. 2 (20), 2022

CONTENTS

Information Technology

Modern Enterprise Management Technologies

Engineering & Industrial Technology

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

UDC 519.863: 330.45 DOI: https://doi.org/10.30837/ITSSI.2022.20.005

V. BESKOROVAINYI, L. KOLESNYK, D.YEVSTRAT

FORMALIZATION OF THE PROBLEM OF TRANSPORT LOGISTICS OPTIMIZATION NETWORKS AT THE STAGE OF REENGINEERING

The **subject** of research in the article is the process of supporting decision-making in the tasks of optimizing closed logistics networks at the stage of reengineering. The **goal** of the work is to improve the efficiency of technologies for the automated design of closed logistics networks due to the improvement of mathematical models of multi-criteria problems of reengineering their topological structures. The following **tasks** are solved in the article: review and analysis of the current state of the problem of supporting decision-making in the tasks of optimizing logistics networks at the stage of their reengineering; decomposition of the problem of optimization of logistics networks at the main stages of their life cycles; selection of a logical scheme of the reengineering process of the logistics network as a territorially distributed object; development of a mathematical model of the general problem of multi-criteria optimization of logistics networks according to indicators of economy, efficiency, reliability and survivability; selection of models for scalar multi-criteria evaluation of reengineering options, taking into account factors that are difficult to formalize, knowledge and experience of the decision-maker. The following **methods** are used: system approach, theories of systems, theories of usefulness, theories of decision-making, system design, optimization and operations research. **Results.** Decomposition of the reengineering problem was carried out on the following tasks: determination of the purpose of reengineering and the principles of network reconstruction; network structure optimization; optimization of the topology of network elements; selection of functioning technology; determination of parameters of elements and vehicles; assessment and selection of the best network construction option. The general mathematical model of the multi-criteria task of reengineering the topological structures of centralized three-level logistics networks based on the indicators of costs, cargo delivery time, reliability and survivability has been improved. Universal functions of general utility and utility of local criteria are proposed to obtain scalar estimates for multiple indicators. Exclusion of part of local criteria and restrictions from the general model allows obtaining models of practically all interesting problems of optimization of logistics networks. **Conclusions.** The developed complex of mathematical models expands the methodological principles of automating the processes of designing logistics networks, allows for the correct reduction of a set of effective options for their construction for the final choice, taking into account factors that are difficult to formalize, the knowledge and experience of designers. The practical use of the proposed complex of mathematical models will reduce the time and capacity complexity of project decision-making support technologies, and due to the use of the proposed options selection procedures, increase their quality based on a number of functional and cost indicators.

Keywords: logistics network; design technology; optimization; reengineering; multi-criteria evaluation; decision support.

Introduction

The efficiency of production and sales processes of modern companies is largely determined by the quality of their logistics, which traditionally covered the processes from the development of sources of raw materials to the supply of finished products to the final consumer [1 - 3]. The next stage in the development of logistics was the management of material, financial and information flows in supply chains. At the same time, one of the more fundamental planning frozen in supply chain management (SCM) is the supply chain network design (SCND) [4]. Under increasing environmental constraints, logistics activities have encompassed the entire cycle from optimal use of raw materials to the disposal of waste activities. The methodology of environmental ("green") logistics is aimed at reducing the risks of environmental degradation and improving the environmental and economic efficiency of companies [5 - 6]. The reversible and closed-loop logistics, which cover the tasks of optimization of reverse inventory, information, money flows, are rapidly developing within the environmental framework [4 - 7].

Changes in the nomenclature and demand for products, location of production facilities and recycling or disposal centers (containers, waste, substandard products, etc.), used vehicles, expansion of the consumer network at a certain stage leads to the need to reengineer existing logistics networks [8]. In general, logistics reengineering involves solving a set of tasks: determining the objectives of the reorganization of the logistics network; identification of operations subject to reengineering; system analysis and development of the reengineering option; evaluation and comparative analysis of the proposed reengineering option; implementation of the reengineering project. At the same time, design and management decisions on reengineering of supply chains (SC) in dynamic business environments should be sufficiently flexible and viable. This, as well as the need to take into account the reverse flows in the processes of closed logistics, generates many new tasks that require system formalization and development of effective methods for their solution [9-10].

Analysis of the current state of the problem and methods of its solution

Reverse and closed-loop logistics are considered one of the effective means of reducing environmental pollution and resource consumption through the recycling and recovery of used products [11 - 13]. At the same time, the theory of optimization of logistics networks with both single and multiple options for recycling or recovery of goods is being developed [14 - 15]. Regardless of the type of structures, networks of both traditional and closed logistics systems usually cover significant areas. Their structural, functional and cost characteristics are largely determined by their topology (location of production, processing, recycling, hubs, and consumers). This feature allows us to classify closed logistics systems into the class of territorially distributed objects [16]. The problem of

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

optimizing such objects belongs to the poorly structured. It contains a set of tasks not fully defined in terms of goals and data, for which no technologies for effective solutions have been designed. The methodology of structural synthesis of such objects is based on the ideas of aggregate-decomposition and block-hierarchical approaches. This involves dividing the description of closed-loop logistics systems into hierarchical levels and aspects, and the optimization process – into groups of procedures related to obtaining and transforming descriptions (solutions) on the selected levels and aspects. Subsequently, the descriptions obtained are combined to receive generalized solutions at the appropriate level.

Traditionally, the optimization problem for such objects is considered as a meta-problem $MetaTask$, the decomposition of which establishes a set of interrelated local problems:

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

where $Task^l$ – set of tasks of the l-th decomposition level; $Task_i^l$ – i-th local task of the l-th level; i_l – number of local tasks at the l-th level; n_l – number of levels of problem decomposition.

At the three-level decomposition scheme (fig. 1), the tasks of system optimization of the logistics network as a territorially distributed design object are distinguished at the macro level [8, 10, 16]. They reflect the features of the main stages of its life cycle and differ only in terms of constraints: $Task_1^1$ – formation of network creation goals and development of the terms of reference for its design; $Task_2^1$ – system design; $Task_3^1$ – network development planning; $Task_4^1$ – network modernization; $Task_5^1$ – network reengineering.

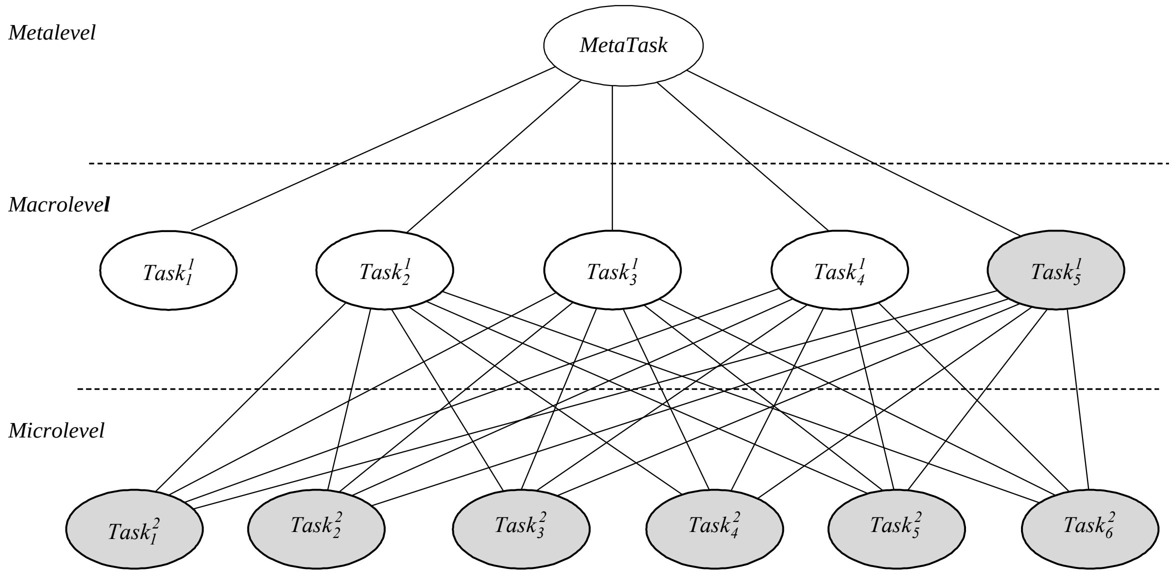


Fig. 1. Decomposition scheme of the logistics network optimization problem as a regionally distributed object [16]

Optimization of transport logistics networks in the process of reengineering at the lower level involves solving a set of interrelated tasks (fig. 1): $Task_1^2$ – determination of reengineering objectives and principles of network reengineering; $Task_2^2$ – optimization of network structure; $Task_3^2$ – optimization of network elements topology (production, processing or recycling points, hubs); $Task_4^2$ – choice of functioning technology; $Task_5^2$ – determination of elements and transport means parameters; $Task_6^2$ – evaluation and choice of the best option of network construction.

In this case, each of the allocated local problem tasks $Task_i^l$, $i = \overline{1, i_l}$ is considered as a transformer of its input data In_i^l into its output data Out_i^l :

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

For an estimation of design decisions the methodology of the functional-cost analysis which assumes a maximization of efficiency of variants of network construction $P(s) \to \max_{s \in S^*}$ (where S^* is a set of admissible variants of network reengineering) is used. For an estimation of efficiency in practice, the ratio of the received effect from use of a network $Q(s)$ and expenses for its achievement $C(s)$ is used [10]:

$$Q(s) = F_1(E,\ R,\ G),\quad C(s) = F_2(E,\ R, G), \quad (3)$$

where $E,\ R,\ G$ – respectively the set of network elements, links between elements and their topologies, determining the locations of the elements; F_1, F_2 – some mappings establishing the dependencies of effect and costs on the characteristics of the network $s = < E,\ R, G >$.

Under the given constraints on the scalar effect $Q(s) \geq Q^*$ and (or) cost $C(s) \leq C^*$ indicators, the

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

problem of reengineering the logistics network is formally presented in the following form:

$$s^o = \arg\max_{S \in S^*}\{[P(s) = Q(s)/C(s)] : Q(s) \geq Q^*, C(s) \leq C\}. \quad (4)$$

Under the condition of a single constraint on the effect $Q(s) \geq Q^*$ or cost $C(s) \leq C^*$ indicators, problem (4) is transformed into the problem of maximizing the effect of using the network under given constraints on resources:

$$s^o = \arg\max_{s \in S^*}(Q(s) : C(s) \leq C^*), \quad (5)$$

or cost minimization under given constraints on the effect of using the network:

$$s^o = \arg\min_{s \in S^*}(C(s) : Q(s) \geq Q^*). \quad (6)$$

Based on the decomposition of the problem (1) and reengineering goal setting and network reengineering principles $Task_1^2$ (4), a network model of the basic problem is created [17]. Based on this model, a logical scheme for obtaining a design solution is created, which will determine the order of solving local tasks of network reengineering $Task_i^2$, $i = \overline{1,6}$. For its construction, a tuple of sets is defined:

$$CirDes = < Tasks, In, Res, DesDec, ProcDec >, \quad (7)$$

where $Tasks = \{Task_i^2\}$, $i = \overline{1,6}$ – ordered set of network reengineering tasks; In – set of task tuple input data $Tasks$; Res – set of task constraints; $DesDec$ – set of options for reengineering the network; $ProcDec$ – a problem-solving procedure that establishes a correspondence between tuples $< In, Res >$ and sets of corresponding design solutions $DesDec$.

At that, the models of each of the logistics network reengineering tasks $Task_i^2$, $i = \overline{1,6}$ are presented in the following form:

$$ModTask_i^2 : \{In_{iE}^2, In_{iI}^2, Res_i^2\} \rightarrow DesDec_i^2, \; i = \overline{1,6}, \quad (8)$$

where In_{iE}^2, In_{iI}^2 – respectively the sets of external and internal with respect to the set of tasks of reengineering of the input data-network $Task_5^1$ of the i-th local task.

For the correct solution of the problems $Task_2^2$, $Task_3^2$, $Task_4^2$, $Task_5^2$ і $Task_6^2$ and information on the solutions of previous problems is used. To obtain it, it is proposed to use an iterative logical scheme that provides for cyclic implementation of procedures for generation, analysis of reengineering options and selection of the best among them (fig. 2).

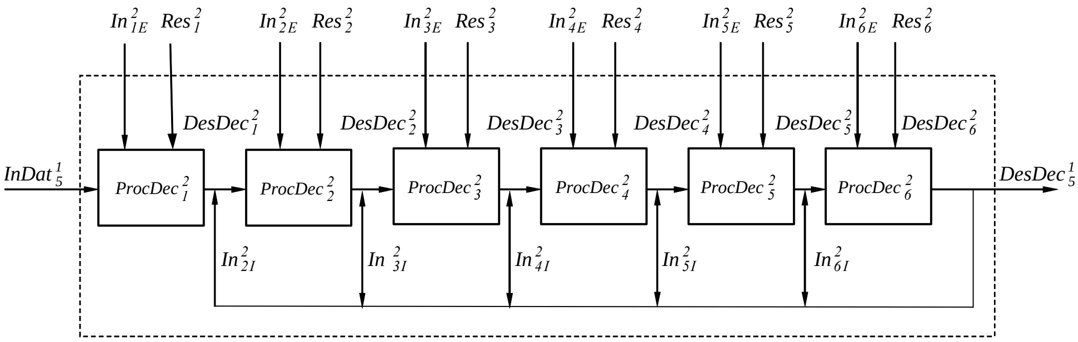


Fig. 2. Iterative logical scheme of reengineering a logistics network as a regionally distributed object [17]

Assessment of the properties of options for reengineering the logistics network is carried out using a set of local cost and functional criteria (cost of goods delivery, time of goods delivery, reliability, survivability of the system, etc.) $K(s) = [k_1(s), k_2(s), ..., k_m(s)]$ [8, 10]:

- costs involved $k_1(s) \rightarrow \min_{s \in S^*}$;
- cargo delivery time: $k_2(s) \rightarrow \min_{s \in S^*}$;
- network reliability (availability factor): $k_3(s) \rightarrow \max_{s \in S^*}$;
- network survivability (share of consumers who receive cargo when its components are damaged): $k_4(s) \rightarrow \max_{s \in S^*}$.

Taking into account the constraints on cost and functional indicators of options mathematical model of multi-criteria problem of optimization of the logistics network is represented in the following form:

$$k_1(s) \longrightarrow \min_{s \in S^*} : k_1(s) \leq k_1^*; \quad k_2(s) \rightarrow \min_{s \in S^*} : k_2(s) \leq k_2^*; \quad k_3(s) \rightarrow \max_{s \in S^*} : k_3(s) \geq k_3^*; \quad k_4(s) \rightarrow \max_{s \in S^*} : k_4(s) \geq k_4^*, \quad (9)$$

where k_1^*, k_2^*, k_3^*, k_4^* – limit acceptable values of cost indicators, responsiveness, reliability and survivability of the logistics network.

To choose the best option of network reengineering from the set of admissible $s^o \in S^*$ in the process of problem solution utility theory models are applied with

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

the use of methods of quantitative or qualitative estimation [18 - 20]. At the same time, it is recommended to remove a subset of dominant (inefficient) variants of network $\bar{S}$ construction from the set of admissible ones [21]. After that, the choice will be made only from the set of effective (Pareto-optimal) options:

$$S^E = S^* \setminus \bar{S}, \quad S^E \cap \bar{S} = \varnothing, \quad S^E \cup \bar{S} = S^*. \qquad (10)$$

The procedure of compilation and selection on small sets of effective network S^E reengineering options is carried out by decision makers (designers) using methods of multicriteria analysis, the most common among which include AHP, MAUT, TOPSIS, PROMETHEE, ELECTRE [22 - 23]. Each of the methods uses a different technology to evaluate decisions, so different variants of reverse engineering can be established as the best. Recently, the comparator identification method, which allows to synthesize a function for quantitative scalar evaluation of the whole set of reengineering variants on the basis of some revealed order on the set of effective variants $P(s)$, $s \in S^E$ has become popular [21, 24].

The most widespread for scalar multicriteria evaluation of options is additive convolution of local criteria using relatively simple functions of their utility [21, 24]:

$$P(s) = \sum_{j=1}^{m} \lambda_j \xi_j(s),$$

$$\xi_j(s) = \{[k_j(s) - k_j^-] / [k_j^+ - k_j^-]\}^{\mu_j}, \qquad (11)$$

where λ_j – coefficients of local criteria importance $k_j(s)$, $j = \overline{1,m}$, $\lambda_j \ge 0$, $\sum_{j=1}^{m} \lambda_j = 1$; $\xi_j(s)$ – value of the utility function of the j-th local criterion for the network reengineering option s; k_j^-, k_j^+, $j = \overline{1,m}$ – the worst and the best value of the j-th criterion on the admissible set of variants S^*; μ_j – the parameter defining a particular kind of function $\xi_j(s)$: concave, convex or linear.

According to the results of the review of the current state of the problem of optimization of transport logistics networks at the stage of reengineering, it was found that:

- the existing models of the problems of reengineering of logistics networks (1) - (8) determine only the relationship of the tasks by variables and parameters and do not allow to obtain quantitative estimates of the options by a variety of functional and cost indicators;

- problems of structural and topological optimization of logistic networks refer to the class of multi-criteria, have combinatorial nature, and the vast majority of options for building networks, analyzed in the process of their solution, are ineffective;

- there is a need to improve mathematical models of structural and topological optimization problems of logistic networks for quantitative assessment of network reengineering options on the set of functional and cost indicators.

In this regard, the aim of the article is to improve the efficiency of automated design technologies of closed logistics networks by improving the mathematical models of multi-criteria problems of reengineering their topological structures.

Research results

Let us consider the problem of optimizing a closed logistics network with integrated centers (production and processing points) according to the four local criteria of economy, efficiency, reliability, and survivability. The indicators of economy and efficiency are traditional in solving the problems of optimization of logistics networks, and the indicators of reliability and survivability are important for military logistics and logistics of critical systems [25].

The problem of reengineering the topological structure of a centralized three-level logistics network is considered in the formulation [8, 10]. Given: the set of elements of the existing network $I = \{i : i = \overline{1,n}\}$; the existing variant of the topological structure of the network $s' \in S^*$, specified by the locations of consumers, nodes, center (coincides with the location of the element $i = 1$), as well as the links between consumers, nodes and center $[s'_{ij}]$ $i, j = \overline{1,n}$ ($s'_{ij} = 1$ if there is a direct connection between the elements i and j and $s'_{ij} = 0$ – if not); the costs of creation (upgrading), operation of nodes c_i, $i = \overline{1,n}$ implementation of transportation c_{ij}, $i, j = \overline{1,n}$, the cost of resources that can be re-used (or sold) after the dismantling of equipment nodes and transport means.

It is necessary to determine the best option in terms of cost, efficiency, reliability and survivability of the topological structure of the logistics network $s^o \in S^*$ (7).

The set of admissible variants of topological structures of the centralized three-level network can be represented in the following way:

$$S = \{s\} = \begin{cases} [s_{ij}], \ s_{ij} \in \{0,1\}, \ i,j = \overline{1,n}, \ s_{11} = 1; \\ \sum_{i=j}^{n} s_{ij} \ge 1, \ \forall j = \overline{1,n}; \\ \sum_{j=1}^{n} \sum_{i=j}^{n} s_{ij} = n + \sum_{i=1}^{n} s_{ii}; \\ s_{ii} = 1 \to s_{i1} = 1 \ \ \forall i = \overline{1,n}; \\ s_{ii} = 1 \wedge s_{ij} = 1 \to ij = \arg \min_{i \le j \le n} c_{ji} \ \ \forall i,j = 1,n. \end{cases} \qquad (12)$$

The main constraints for a three-level centralized network, presented in conditions (12): each consumer in the network must be connected to one of the nodes or directly to the center; more than one consumer must be

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

directly connected to each node; each consumer i is connected to terminal j by an indicator of minimum reduced costs; each of the nodes in network j has a direct connection to the center; the number of nodes in the network is in the range $1 \le \sum_{i=j}^{n} s_{ii} \le n/2$; total number of direct connections in the network structure is $\sum_{j=1}^{n}\sum_{i=j}^{n} s_{ij} = n + \sum_{i=1}^{n} s_{ii}$.

The local criterion for the cost of reengineering the logistics network in the above designations can be represented in the following form:

$$k_1(s', s) = \sum_{i=1}^{n} [c_i(1-s'_{ii})\, s_{ii} + d_i s'_{ii} s_{ii} + e_i(1-s_{ii})\, s'_{ii} - g_i(1-s_{ii})\, s'_{ii}] + \\ + \sum_{j=1}^{n}\sum_{i=j}^{n} [c_{ij}(1-s'_{ij})\, s_{ij} + d_{ij} s'_{ij}\, s_{ij} + e_{ij}(1-s_{ij})\, s'_{ij} - g_{ij}(1-s_{ij})\, s'_{ij}] \to \min_{s \in S^*}, \quad (13)$$

where c_i – the cost of creating a i-th consumer-based node; $i = \overline{1,n}$; s'_{ij}, s_{ij} – elements of the matrices of connections between elements in the existing network $s' = [s'_{ij}]$ and in the network structure after reengineering $s = [s_{ij}]$; d_i – given the cost of upgrading a i-th consumer-based node; e_i – the cost of removing a i-th consumer-based node in the existing network; g_i – the cost of resources that can be reused after the removal of i-th consumer-based node equipment; c_{ij} – the given cost of transporting goods between elements i and j, $i, j = \overline{1,n}$.

The local efficiency criterion for a three-tiered centralized network defines the maximum delivery time to the entire set of consumers:

$$k_2(s) = [\max_i \sum_{i=1}^{n} \tau_{1i} s_{1i} + \max_i \sum_{i=1}^{n} \tau_i s_{ii} + \max_{i,j} \sum_{i=1}^{n}\sum_{i=1}^{n} \tau_{ij} s_{ij}] \to \min_{s \in S^*}, \quad (14)$$

where τ_{1i} – time of cargo transportation from the production center to the node at the base of the i-th consumer; τ_i – time of cargo handling at the node at the base of the i-th consumer; τ_{ij} – time for cargo delivery from the node at the base of the i-th consumer to the j-th consumer.

When assessing the reliability of logistics network options, we take into account the reliability of production equipment, node equipment, and vehicles in use. We will assume that the equipment of the nodes of the logistics network and the vehicles used have the same reliability. In the local reliability criterion, we propose to use the coefficient of network availability for the full performance of the function of cargo delivery:

$$k_3(s) = h_1 \times (h_2)^{u(s)} \times (h_3)^{u(s)} \times (h_4)^n \to \max_{s \in S}, \quad (15)$$

where h_1, h_2, h_3, h_4 – availability coefficients of the equipment of the center, node, transport means used between the center and nodes, as well as between the nodes and consumers; $u(s) = \sum_{i=1}^{n} s_{ii}$ – number of nodes in the network.

When estimating the survivability, we will assume that the consumers of the logistics network receive approximately the same amount of cargo (have approximately the same weight for the sender). While estimating the survivability of the network, we can use the value of the share of consumers receiving cargoes in case of single damage of its components. In this case irrespective of the topological structure of the network, when the center equipment is damaged $k_4(s) \equiv 0$, and when a single vehicle is damaged between the nodes and the end users $k_4(s) \equiv (n-1)/n$. From the point of view of survivability, the damage of a node causes the same network losses as the damage of the vehicle between the center and the node. Considering this, the survivability maximization criterion, taking into account the damage of the vehicle between the center and the nodes, as well as the node equipment, can be represented in the following form:

$$k_4(s) = \left\{ \min_{1 \le j \le n} \left\{ (n - \sum_{j=2}^{n}\sum_{i=j}^{n} s_{ji} s_{ii}) / n \right\} \right\} \to \max_{s \in S}. \quad (16)$$

To estimate the values of local criteria, we use the most effective in terms of the complex indicator "accuracy-complexity" function that allows to reproduce not only linear, but also non-linear, including *S*- and *Z*-shaped approximations. [21]:

$$\xi(s) = \begin{cases} \bar{a}(b_1+1)\left(1-\left(b_1 / \left(b_1 + \dfrac{\bar{k}(s)}{\bar{k}_a}\right)\right)\right), 0 \le \bar{k}(s) \le \bar{k}_a; \\ \bar{a} + (1-\bar{a})(b_2+1)\left(1-\left(b_2 / \left(b_2 + \dfrac{\bar{k}(s) - \bar{k}_a}{1-\bar{k}_a}\right)\right)\right), \bar{k}_a < \bar{k}(s) \le 1, \end{cases} \quad (17)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

where $\xi(s) = \bar{k}(s)$; $\bar{k}_a, \bar{a}$ – coordinates of the glue point of the function, $0 \le \bar{k}_a \le 1$, $0 \le \bar{a} \le 1$; b_1, b_2 – parameters determining the type of dependence on the two segments of the function

To quantify the overall usefulness of options for reengineering logistics networks on the four indicators, we will use a universal function constructed using the Kolmogov-Gabor polynomial [21, 24]:

$$P(s) = \sum_{i=1}^{4} \lambda_i \xi_i(s) + \sum_{i=1}^{4}\sum_{j=i}^{4} \lambda_{ij}\xi_i(s)\xi_j(s) + \sum_{i=1}^{4}\sum_{j=i}^{4}\sum_{l=j}^{4} \lambda_{ijl}\xi_i(s)\xi_j(s)\xi_l(s) + \sum_{i=1}^{4}\sum_{j=i}^{4}\sum_{l=j}^{4}\sum_{k=l}^{4} \lambda_{ijlk}\xi_i(s)\xi_j(s)\xi_l(s)\xi_k(s), \quad (17)$$

where λ_i, λ_{ij}, λ_{ijl}, λ_{ijlk} – weighting coefficients assessing the mutual importance of the criteria $k_i(s)$, $k_j(s)$, $k_l(s)$, $k_k(s)$ and their products; $0 < \xi_i(s) < 1$, $i = \overline{1,m}$ – value of the utility function of the local criterion $k_i(s)$, $i = \overline{1,m}$ (17) for the option $s \in S^E$.

It is proposed to solve the problem of optimizing the logistics network using the combined method [21].

In the framework of this method, it is proposed not to form a set of admissible options for reengineering S^*, but in the process of generation using modifications of the directed search method to form a subset of effective options S^E at once. The total number of possible variants of topological structures in the reengineering of a three-level centralized network for the number of terminals $1 < u \le n/2$ is [8]:

$$N(n) = \frac{1}{2}\sum_{u=1}^{n} C_n^u = \frac{1}{2}\sum_{u=1}^{n} \frac{n!}{u!(n-l)!} = 2^n / 2, \quad (16)$$

where n – the number of places of possible placement of nodes (network consumers).

Thus, the quantity of effective variants is essentially less and their share decreases with the growth of dimensionality of the problem (tab. 1, fig. 3 - 4). Due to the significant reduction of variants, subject to the analysis, it allows to significantly reduce the time of solving the problem. Next, on the set of effective variants S^E, let us define a subset of variants $S' \subseteq S^E$ for preliminary estimation by designers [21]. On it with the use of comparator identification technology we will carry out a structural-parametric synthesis of the function of the total utility of the variants $P(s)$. This will allow based on the values $P(s)$ to carry out the ranking of options from the set of effective S^E and provide the necessary number of them for the final choice of the decision maker.

Table 1. *Capacities of a subset of effective logistics network reengineering options for* $m = 4$

$\lvert S^*\rvert$	10000	20000	30000	40000	50000	60000	70000	80000	90000	100000
$\lvert S^E\rvert$	151	195	216	253	268	281	298	302	329	342
$\lvert S^E\rvert / \lvert S^*\rvert$	0,0151	0,0098	0,0072	0,0063	0,0054	0,0047	0,0043	0,0038	0,0037	0,0034

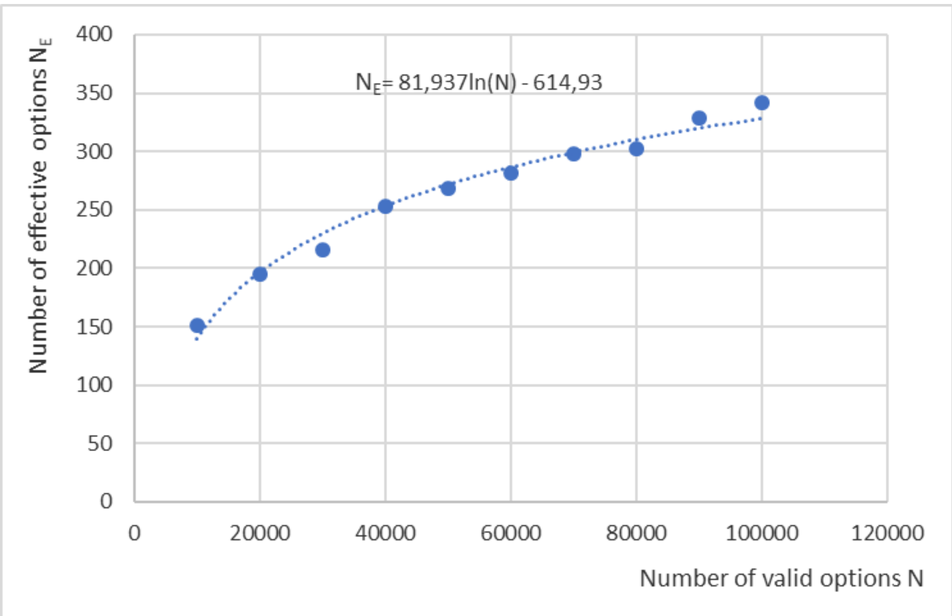


Fig. 3. Relative number of effective network options for $m = 4$

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

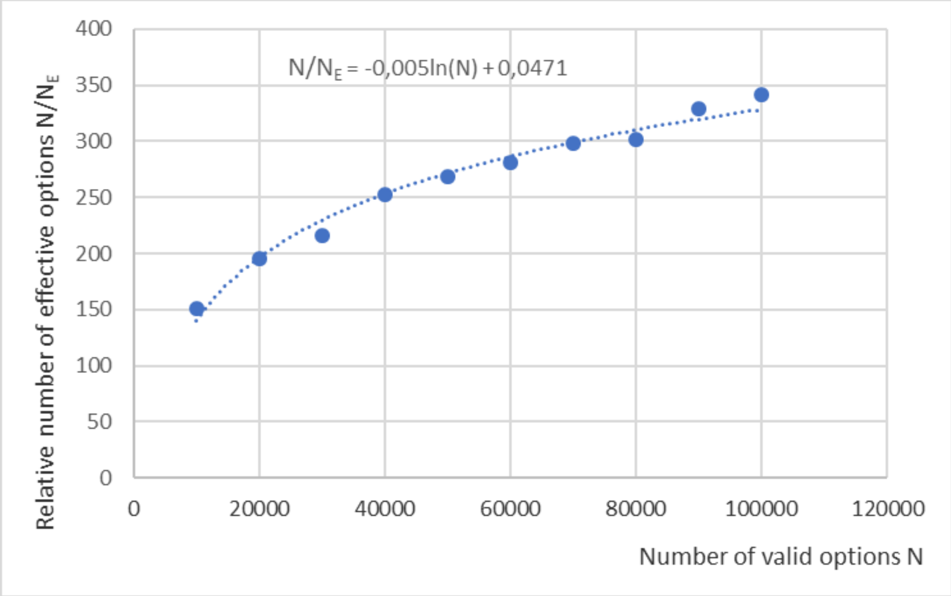


Fig. 4. Relative number of effective network options for $m = 4$

Based on the dimensionality of the network using the obtained approximation of the dependence of the power of the multiple number of effective options on the number of valid options (fig. 3), taking into account relation (16), we can choose the best method for solving the problem of its reengineering. This will allow to obtain the most effective options for reengineering of logistics networks, taking into account the available time and computing resources involved in design automation systems.

Conclusions

In the framework of the methodology of the system approach, closed logistics networks are considered as typical territorially distributed objects, the design tasks of which are combinatorial in nature and are solved by a variety of cost and functional indicators in conditions of incomplete certainty of goals and data. Significant costs of creation and operation of logistics networks need a perfect methodology of their optimization. In order to expand the capabilities of existing models of the problem of optimization of logistics networks, their improvement is proposed. The decision of the problem is made with the use of methodology of aggregative-decomposition approach that allows to carry out its analysis on meta-, macro- and microlevels. The optimization procedures, defined in this way, have been formalized for the complexes of tasks, related to the main stages of the life cycles of networks. They allow to obtain and transform task descriptions with their subsequent aggregation to obtain the best option of network reengineering.

On this basis, to optimize the network at the stage of reengineering, an iterative logical scheme of reengineering is chosen, which allows to jointly solve the entire set of problems and cyclically refine the data for subsequent tasks by the results of the previous ones. A general mathematical model of the multi-criteria problem of reengineering of topological structures of centralized three-tier logistics networks by the indicators of reduced costs, cargo delivery time, reliability and survivability has been improved. In order to obtain scalar estimates for the set of characteristics, universal functions of general utility and utility of local criteria are used. Excluding a part of local criteria and restrictions from the general model, it is possible to obtain models of all practically interesting problems of optimization of logistic networks. The models are proposed to be used in a combined method of options ranking for the final choice by a decision maker. This method, unlike traditional ones, implies formation rather than allocation of a subset of effective options, parametric synthesis of the general utility function and ranking of options according to the results of quantitative assessment. The developed complex of mathematical models extends methodological bases of automation of processes of optimization of logistic networks, allows to carry out correct reduction of a set of effective variants of their construction for a final choice taking into account knowledge and experience of designers that are difficult to formalize. Practical use of the offered complex of mathematical models will allow to lower time and capacity complexity of technologies of support of acceptance of design decisions, and at the expense of use of the offered procedures of selection of variants - to raise their quality on a set of functional and cost parameters. Further research in this direction can be directed at taking into account in the models of optimization of logistic networks the incomplete certainty of goals and input data, using the apparatus of interval or fuzzy analysis, as well as the development of more effective methods for their optimization.

References

1. Horbenko, I. D., Horbenko, Yu. I. (2012), *Applied cryptology: monograph* [*Prykladna kryptolohiia: monohrafiia*], Kharkiv: Kharkiv National University of Radio Electronics, LLC "Fort", 868 p.

2. Bevz, O. M., Kvєtnii, R. N. (2010), *Data Encryption Based on Highly Nonlinear Boolean Functions and Maximum Distance Codes:* monograph [*Shyfruvannia danykh na osnovi vysoko neliniinykh bulevykh funktsii ta kodiv z maksymalnoiu vidstanniu*: monohrafiia], Vinnytsia: Vinnytsia National University of Technology, 96 p.
3. Manifavas, C., Hatzivasilis, G., Fysarakis, K., Rantos, K. (2012), "Lightweight cryptography for embedded systems a comparative analysis", *In: 6th International Workshop on Autonomous and Spontaneous Security SETOP 2012, Springer, LNCS, 8247,* P. 333–349. **DOI:** https://doi.org/10.1007/978-3-642-54568-9_21
4. Gildas Avoine, Julio Hernandez-Castro (2021), "Security of Ubiquitous Computing Systems", *Selected Topics. Springer*, P. 265 **DOI:** https://doi.org/10.1007/978-3-030-10591-4
5. Biryukov Alex and Perrin Leo (2017), "State of the art in lightweight symmetric cryptography", *Cryptology ePrint Archive, Report 2017/511,* available at: http://eprint.iacr.org/2017/511, https://eprint.iacr.org/2017/511.pdf
6. Mitsuru Matsui (1997), "New block encryption algorithm MISTYC", *In Eli Biham, editor, Fast Software Encryption – FSE'97, pringer, volume 1267 of Lecture Notes in Computer Science, Haifa, Israel, January 20–22,* P. 54–68, available at: https://link.springer.com/chapter/10.1007/BFb0052334
7. Hatzivasilis George, Fysarakis Konstantinos, Ioannis (2018), "Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers", *Cryptographic Engineering,* No. 8 (2), P. 141–184. **DOI:** https://doi.org/10.1007/s13389-017-0160-y
8. Kerry A. McKay, Larry Bassham, Meltem Sonmez Turan, and Nicky Mouha (2016), "Nistir 8114 - report on lightweight cryptography". **DOI:** https://doi.org/10.6028/NIST.IR.8114
9. Rudnytsky, V. M., Lada, N. V., Babenko, V. G. (2018), *Cryptographic coding: synthesis of stream encryption operations with accuracy to permutation: monograph* [*Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky: monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 184 p.
10. Rudnitsky, V. M., Milchevich, V. Ya., Babenko, V. G., Melnyk, R. P., Rudnitsky, S. V., Melnyk O. G. (2014), *Cryptographic coding: methods and means of implementation (part 2):* monograph [*Kriptograficheskoe kodirovanie: metody i sredstva realizacii (chast' 2):* monografiya], Monograph, Kharkov: Publishing house "Shchedra sadyba plius", 223p.
11. Rudnytsky, V. M., ed. (2018), *Cryptographic coding: information processing and protection: collective monograph* [*Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kolektyvna monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 139p.
12. Sysoienko, S., Myronets, I., Babenko, V. (2019), "Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation", *Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), CEUR Workshop Proceedings 2353, CEUR-WS.org,* P. 402–412. (Scopus) available at: http://ceur-ws.org/Vol-2353/, http://ceur-ws.org/Vol-2353/paper32.pdf
13. Rudnitsky, V., Berdibayev, R., Breus, R., Lada, N. and Pustovit, M. (2019), "Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation", *Advanced Information Systems, Kharkiv: NTU "KhPI",* No. 3 (4), P. 109–114. **DOI:** http://doi.org/10.20998/2522-9052.2019.4.16
14. Lada, N. V., Kozlovska, S. G., Rudnitsky, S. V. (2019), " The symmetric operations' mathematical group constructing based on module-2 addition " ["Pobudova matematy`chnoyi grupy` sy`metry`chny`x operacij na osnovi dodavannya za modulem dva"]. *Modern special technics: scientific and practical journal. Kyiv,* No 4 (59), P.33–41.
15. Lada, N. V., Kozlovska, S. G. and Rudnitskaya, Y. V. (2019), "Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii dodavannia za modulem chotyry "], *Central Ukrainian Scientific Bulletin. Technical Sciences,* No. 2 (33), P. 181–189. **DOI:** http://doi.org/10.32515/2664-262x. 2019.2(33)
16. Lada, N. V., Rudnitsky, S. V., Zazhoma, V. M. and Rudnytska, Y. V. (2020), " Research and synthesis of a group of symmetric modified operations of right-handed addition by module four" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii pravostoronnoho dodavannia za modulem chotyry"], *Control, Navigation and Communication Systems. Academic Journal. Poltava: PNTU,* No. 1 (59), P. 93–96. **DOI:** https://doi.org/10.26906/SUNZ.2020.1.093
17. Rudnitsky, V. M., Babenko, V. G., Rudnitsky, S. V. (2012), " Method of synthesis of matrix models of operations of cryptographic recoding of information" ["Metod syntezu matrychnykh modelei operatsii kryptohrafichnoho perekoduvannia informatsii"], *Ukrainian Information Security Research Journal,* Vol 14, No. 3 (56), P. 50–56. **DOI:** https://doi.org/10.18372/2410-7840.14.3360

Received 18.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Безкоровайний Володимир Валентинович – доктор технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри системотехніки, Харків, Україна; e-mail: vladimir.beskorovainyi@nure.ua; ORCID: https://orcid.org/0000-0001-7930-3984.

Бескоровайный Владимир Валентинович – доктор технических наук, профессор, Харьковский национальный университет радиоэлектроники, профессор кафедры системотехники, Харьков, Украина.

Beskorovainyi Vladimir – Doctor of Sciences (Engineering), Professor, Kharkiv National University of Radio Electronics, Professor of the Department of System Engineering, Kharkiv, Ukraine.

Колесник Людмила Володимирівна – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри системотехніки, Харків, Україна; e-mail: liudmyla.kolesnyk@nure.ua; ORCID: https://orcid.org/0000-0003-4417-7759.

Колесник Людмила Владимировна – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры системотехники, Харьков, Украина.

Kolesnyk Lyudmyla – Candidate of Technical Sciences, Associate Professor, Kharkiv National University of Radio Electronics, Professor of the Department of System Engineering, Kharkiv, Ukraine.

Євстрат Дмитро Іванович – кандидат технічних наук, доцент, Харківський національний економічний університет ім. Семена Кузнеця, доцент кафедри інформаційних технологій, Харків, Україна; e-mail:dmitry.yevstrat@gmail.com; ORCID: https://orcid.org/0000-0001-8393-6063.

Евстрат Дмитрий Иванович – кандидат технических наук, доцент, Харьковский национальный экономический университет им. Семёна Кузнеца, доцент кафедры информационных технологий, Харьков, Украина.

Yevstrat Dmytro – Candidate of Technical Sciences, Associate Professor, Kharkiv National Economics University Simon Kuznets, Associate Professor, Department of Information Systems, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20) ISSN 2524-2296 (online)

ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ОПТИМІЗАЦІЇ МЕРЕЖ ТРАНСПОРТНОЇ ЛОГІСТИКИ НА ЕТАПІ РЕІНЖИНІРИНГУ

Предметом дослідження в статті є процес підтримки прийняття рішень в задачах оптимізації замкнених логістичних мереж на етапі реінжинірингу. **Мета** роботи – підвищення ефективності технологій автоматизованого проектування замкнених логістичних мереж за рахунок удосконалення математичних моделей багатокритеріальних задач реінжинірингу їх топологічних структур. У статті вирішуються наступні **завдання:** огляд і аналіз сучасного стану проблеми підтримки прийняття рішень в задачах оптимізації логістичних мереж на етапі їх реінжинірингу; декомпозиція проблеми оптимізації логістичних мереж на основних етапах їх життєвих циклів; вибір логічної схеми процесу реінжинірингу логістичної мережі як територіально розподіленого об’єкта; розробка математичної моделі загальної задачі багатокритеріальної оптимізації логістичних мереж за показниками економічності, оперативності, надійності та живучості; вибір моделей для скалярного багатокритеріального оцінювання варіантів реінжинірингу з урахуванням факторів, що важко піддаються формалізації, знань і досвіду особи, що приймає рішення. Використовуються такі методи: системний підхід, теорії систем, теорії корисності, теорії прийняття рішень, системного проєктування, оптимізації та дослідження операцій. **Результати.** Виконана декомпозиція проблеми реінжинірингу на задачі: визначення мети реінжинірингу та принципів перебудови мережі; оптимізації структури мережі; оптимізації топології елементів мережі; вибору технології функціонування; визначення параметрів елементів і транспортних засобів; оцінки та вибору найкращого варіанту побудови мережі. Удосконалено загальну математичну модель багатокритеріальної задачі реінжинірингу топологічних структур централізованих трирівневих логістичних мереж за показниками наведених витрат, часу доставки вантажів, надійності та живучості. Для отримання скалярних оцінок за множиною показників запропоновано універсальні функції загальної корисності і корисності локальних критеріїв. Виключення частини локальних критеріїв та обмежень із загальної моделі дозволяє отримувати моделі всіх практично цікавих задач оптимізації логістичних мереж. **Висновки.** Розроблений комплекс математичних моделей розширює методологічні засади автоматизації процесів проєктування логістичних мереж, дозволяє здійснювати коректне скорочення множини ефективних варіантів їх побудови для остаточного вибору з урахуванням факторів, що важко піддаються формалізації, знань і досвіду проєктувальників. Практичне використання запропонованого комплексу математичних моделей дозволить знизити часову й ємнісну складності технологій підтримки прийняття проєктних рішень, а за рахунок використання запропонованих процедур відбору варіантів – підвищити їх якість за множиною функціональних і витратних показників.

Ключові слова: логістична мережа; технологія проєктування; оптимізація; реінжиніринг; багатокритеріальне оцінювання; підтримка прийняття рішень.

ФОРМАЛИЗАЦИЯ ПРОБЛЕМЫ ОПТИМИЗАЦИИ СЕТЕЙ ТРАНСПОРТНОЙ ЛОГИСТИКИ НА ЭТАПЕ РЕИНЖИНИРИНГА

Предметом исследования в статье является процесс поддержки принятия решений в задачах оптимизации замкнутых логистических сетей на этапе реинжиниринга. **Цель** работы – повышение эффективности технологий автоматизированного проектирования замкнутых логистических сетей за счет усовершенствования математических моделей многокритериальных задач реинжиниринга их топологических структур. В статье решаются следующие **задачи:** обзор и анализ современного состояния проблемы поддержки принятия решений в задачках оптимизации логистических сетей на этапе их реинжиниринга; декомпозиции проблемы оптимизации логистических сетей на основных этапах их жизненных циклов; выбор логической схемы процесса реинжиниринга логистической сети как территориально распределенного объекта; разработка математической модели общей задачи многокритериальной оптимизации логистических сетей по показателям экономичности, оперативности, надежности и живучести; выбор моделей для скалярной многокритериальной оценки вариантов реинжиниринга с учетом трудноформализуемых факторов, знаний и опыта лица, принимающего решения. Используются следующие **методы:** системный подход, теории систем, теории полезности, теории принятия решений, системного проектирования, оптимизации и исследования операций. **Результаты.** Выполнена декомпозиция проблемы реинжиниринга на задачи: определения цели реинжиниринга и принципов перестройки сети; оптимизации структуры сети; оптимизации топологии элементов сети; выбора технологии функционирования; определения параметров элементов и транспортных средств; оценки и выбора наилучшего варианта построения сети Усовершенствована общая математическая модель многокритериальной задачи реинжиниринга топологических структур централизованных трехуровневых логистических сетей по показателям приведенных затрат, времени доставки грузов, надежности и живучести. Для получения скалярных оценок по множеству показателей предложены универсальные функции общей полезности и полезности локальных критериев. Исключение части локальных критериев и ограничений из общей модели позволяет получать модели всех практически интересных задач оптимизации логистических сетей. **Выводы.** Разработанный комплекс математических моделей расширяет методологические основы автоматизации процессов проектирования логистических сетей, позволяет осуществлять корректное сокращение множества эффективных вариантов их построения для окончательного выбора с учетом трудно поддающихся формализации знаний и опыта проектировщиков. Практическое использование предлагаемого комплекса математических моделей позволит снизить временную и емкостную сложности технологий поддержки принятия проектных решений, а за счет использования предложенных процедур отбора вариантов – повысить их качество по множеству функциональных и затратных показателей.

Ключевые слова: логистическая сеть; технология проектирования; оптимизация; реинжиниринг; многокритериальная оценка; поддержка принятия решений.

Бібліографічні описи / Bibliographic descriptions

Безкоровайний В. В., Колесник Л. В., Євстрат Д. І. Формалізація проблеми оптимізації мереж транспортної логістики на етапі реінжинірингу. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 5–13. DOI: https://doi.org/10.30837/ITSSI.2022.20.005

Beskorovainyi, V., Kolesnyk, L., Yevstrat, D. (2022), "Formalization of the problem of transport logistics optimization networks at the stage of reengineering", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 5–13. DOI: https://doi.org/10.30837/ITSSI.2022.20.005

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 004.9: 519.81 DOI: https://doi.org/10.30837/ITSSI.2022.20.014

V. BESKOROVAINYI, L. KOLESNYK, M. ALOKHINA, V. KOSENKO

DETERMINING PREFERENCES IN RECOMMENDER SYSTEMS BASED ON COMPARATOR IDENTIFICATION TECHNOLOGY

The **subject** of research in the article is the process of ranking objects in the lists of recommender systems. The **goal** of the work is to increase the efficiency of recommender systems by improving the method of determining preferences between objects in lists using the theory of multi-criteria decision-making. The following **tasks** are solved in the article: review and analysis of the current state of the problem of identifying advantages between objects and their ranking in the lists of recommender systems; analysis of filtering methods used in recommendation systems; decomposition of the decision support problem for selection of objects; development of a combined method for ranking objects in the lists of recommender systems, combining the procedures for selecting a subset of Pareto-optimal objects, structural-parametric synthesis of a scalar multi-criteria estimation model, and evaluating the entire set of selected objects. The following **methods** are used: mathematical modeling, systems theory, utility theory, decision theory, optimization and operations research. **Results.** Based on the results of the analysis of the modern methodology for ranking objects in the lists of recommendation systems, the possibility of increasing their efficiency has been established. To take into account factors difficult to formalize, the knowledge and experience of users, it is proposed to implement the determination of preferences between objects using the theory of multi-criteria decision making. The problem of forming lists of recommendation systems is decomposed into the tasks of selecting a subset of Pareto-optimal objects, structural-parametric synthesis of a scalar multi-criteria estimation model, and evaluating a set of selected objects. A combined method for ranking options has been developed that combines the procedures of ordinalistic and cardinalistic ordering technologies and allows one to correctly reduce the subsets of objects included in the lists of recommendations. Conclusions. The developed method for determining preferences expands the methodological foundations for automating the development and operation of recommendation systems, other multi-criteria decision support systems, allows for the correct reduction of the set of non-dominated objects for the final choice, taking into account factors that are difficult to formalize, knowledge and user experience. The practical use of the obtained results due to more economical method of forming lists when adding new objects will allow to decrease the time and capacity complexity of the procedures for providing recommendations, and due to taking into account of set of weighted local indexes and allocation of set of non-dominated objects - to increase quality of given recommendations.

Keywords: multi-criteria assessment; comparator identification; recommender system; ranking of objects; structural-parametric synthesis.

Introduction

One of the modern trends is the rapid growth of the range and volume of goods and services sold in the market. On the one hand, this allows to better meet the needs of consumers, but significantly complicates for them the task of choosing the object (goods, services, leisure facilities, etc.) that best meets their preferences. In cases when a lot of objects of choice are offered, it creates a potential problem for Internet users [1]. To avoid information overload, consumers need to properly filter objects, prioritize them, and provide relevant information about them. To simplify consumers' choices, recommendation systems are increasingly being used to solve this problem by searching through a large volume of dynamically received information. Due to the use of filtering methods, they allow providing users with the necessary personalized information about the objects that most correspond to their preferences [2].

The information about the similarity of the characteristics of objects or about the acts of selection of objects by users with similar preferences is used for the formation of suggestions in recommendation systems. The most widespread methods for solving the problems of recommendation formation in them are methods of collaborative filtering, recommendations based on content and knowledge [3 - 5]. Their main disadvantage is the high complexity of debugging or use, which creates problems when it is necessary to analyze information from powerful sets of objects for a large number of users. In addition, these methods are focused on the formation of recommendations using generalized evaluations of objects. To improve the accuracy of establishing user preferences, the use of multicriteria decision-making models and methods looks promising [6 - 9]. In this case, it is reasonable to justify a scalar criterion of choice, which would sufficiently fully characterize objects on the basis of some set of contradictory local criteria [10-11]. When decision-making technologies are used in recommender systems, the evaluation of the effectiveness of objects can be performed on the basis of utility theory using methods of individual or collective expert evaluation [12 - 14]. In recommendation systems, their users act as professionals. To form recommendation lists using decision theory, it is necessary to identify a subset of Pareto-optimal objects on the set of admissible objects by local criteria, parametric synthesis of their scalar evaluation model, and calculation of their generalized evaluations. To implement these tasks it is necessary to develop appropriate mathematical models and effective methods for their solution.

Analysis of the problem and methods of its solution

Modern recommender systems use explicit (when the user is asked to perform certain evaluations) and implicit (when information is obtained without the user performing evaluation actions) methods of information collection. In the first case, the user makes a quantitative assessment of objects, their ranking, determines the best among the whole set or proposed pairs of objects. In the second case, information about the user's interest in the content of the network, their subscriptions, messages, location, etc. is analyzed. Collaborative filtering first came into use as a

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

means of combating excessive information on the Internet, and later filtering systems began to emerge that could automatically identify relevant opinions and aggregate them to provide recommendations. In the simplest case, personalized recommendations are presented as ranked lists of items [15].

One of the key problems of recommender systems is considered a problem of cold start [16]. Such a problem occurs in situations of incomplete data regarding preferences or selection of objects by new users or users who do not regularly perform automated selection of objects (purchase of real estate, vehicles, selection of tourist objects, etc.). The cold start problem is usually solved in two steps: context analysis of the input data and collaborative filtering. The context analysis process uses user behavior characteristics, which can be constructed using gradient descent and represented in the form of temporal graphs or neural network models [5]. A disadvantage of most recommendation systems is considered to be the use of only filters and sorting by user evaluation without taking into account user's individual preferences. More effective is the technology of collaborative filtering, which involves the analysis of object ratings received from users with similar preferences.

In traditional formulations of the problem of providing recommendations the set of system users $U=\{u_j\}$, $j=\overline{1,m}$ and objects of choice are considered set $O=\{o_i\}$, $i=\overline{1,n}$. In the process of interaction with the recommendation system, users provide information for forming a matrix of selection objects' ratings $R=[r_{ij}]$, $i=\overline{1,n}$, $j=\overline{1,m}$ (where r_{ij} is object $o_i \in O$ rating of user's $u_j \in U$. Taking into account that the number of objects in modern recommendation systems can be large, and known objects constitute a rather insignificant fraction of them, in practice the matrices of certain ratings $R'=[r_{ij}]$ are usually highly sparse. The main function of such systems is the establishment of prediction and recommendation for users about new objects. Such predictions can be represented by orders, binary relations or numerical values P_{ji} reflecting the value of the whole set of objects $o_i \in O$, $i=\overline{1,n}$ for users $u_j \in U$, $j=\overline{1,m}$. In this case, the recommendation is a list of the most preferred objects for a particular user. In this case, the recommendation is a list of the $N=|O'|$ objects $O' \subseteq O$ most suitable for a particular user.

In practice, it often turns out that a significant number among the objects proposed as alternatives may be ineffective under Pareto [17-18] in their multicriteria evaluation.

Orders on the set of recommended objects can be presented in the following form:

$$o_i \succ o_j \succ \ldots \succ o_z, \quad o_i, o_j, \ldots, o_z \in O' \subseteq O. \qquad (1)$$

A binary strict advantage relation reflecting the relative value of user objects can be represented as a set of arranged pairs:

$$R(O')=\{<o_i, o_j>: \ o_i, o_j \in O', \ o_i \succ o_j\}. \qquad (2)$$

Most modern recommender systems use only filters and sorting based on the user's score, without taking into account the user's individual preferences. To overcome this drawback, the technology of collaborative filtering is used. It analyzes the ratings of objects given by users with similar preferences (fig. 1) [19]. Due to the sparseness of matrices $R'=[r_{ij}]$ and their high dimensionality (as a result of the growth of the volume of information regarding objects and users), the use of this method in many cases is irrational. In such cases, for practical implementation of collaborative filtering technology it is reasonable to use graph data model. In it, the results are represented as sets consisting of "user-object" pairs $u_j \times o_i$, $j=\overline{1,m}$, $i=\overline{1,n}$. Then for the predicted estimates, each pair of $u_j \times o_i$, $j=\overline{1,m}$ $i=\overline{1,n}$ will correspond the value of the predicted user estimate.

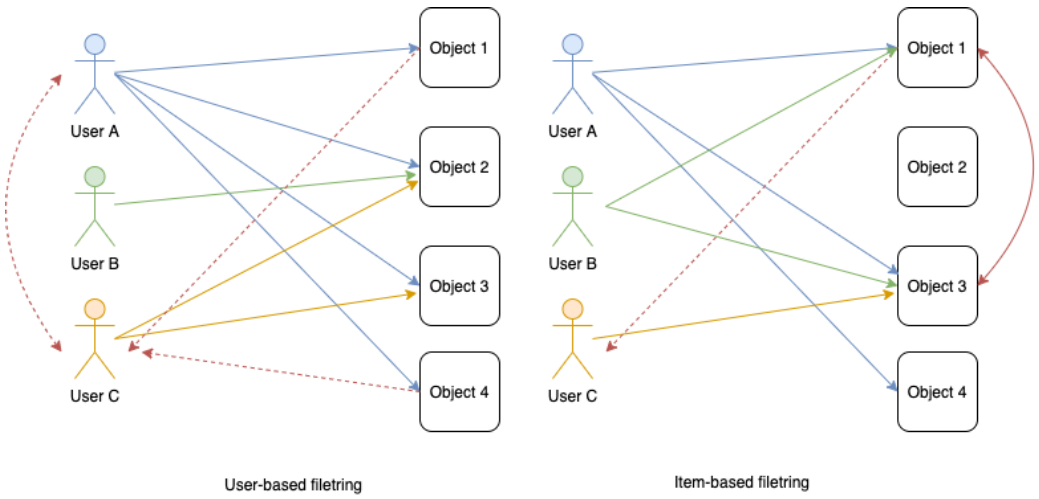


Fig. 1. Schemes of approaches based on the neighborhood of users and objects [19]

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

In the projected graph of links

$$G = (V = (U, O'), E). \quad (3)$$

Vertices are elements from the sets $U = \{u_j\}$ and $O' = \{o_i\}$, and the edges E are set by the corresponding tuples $< u_j \in U, o_i \in O' >$, $j = \overline{1,m}$, $i = \overline{1,n}$.

The presence of an arc between the vertices of the graph u_j and o_i means that the object $o_i \in O'$ will be recommended (given a predictive score) to the user $u_j \in U$. Each arc of the graph has a weight corresponding to the value of the "user-object" distance function $d_{UO} = L(u_j \in U, o_i \in O')$.

Each vertex of the graph (3) corresponding to the preferences of an individual system user $u_j \in U$ has a certain number of arcs connecting it with the vertices corresponding to different objects of choice $o_i \in O'$. It is equal to the number of recommendations (or forecasts) requested by the user. Then the development of user's prediction is reduced to finding such a graph of connections, which will have the minimal weight of all arcs. This will correspond to the recommendation of such objects of choice for the user, in the graph of links the average distance between the vertices corresponding to them and the user will be the least.

A review of the current state of the problem of determining benefits in recommender systems found that:

- recommender systems are most likely to be useful to users who do not have sufficient personal experience or competence to evaluate alternative facilities and the reliance on recommendations from other users of the system;
- a significant number among facilities that are offered as alternatives may be ineffective under Pareto;
- content-based recommendations identify similarities in features of object content, but have a strong dependence on subject matter and limited value of recommendations;
- collaborative filtering is a generic approach, it generally produces better results than content-based filtering, but has a cold-start problem in the absence of information about user preferences;
- knowledge-based recommendations are of the highest quality, but the development and use of such systems is expensive;
- in its essence, recommender systems are specific decision support systems, to improve their effectiveness, the use of models and methods of multi-criteria decision making looks promising.

The aim of the study is to improve the effectiveness of recommender systems by improving the method for determining the advantages between objects in lists using the theory of multicriteria decision-making.

Results of the study

To increase the accuracy of user advantage determination, we use a mathematical apparatus to determine on the set of acceptable subsets of Pareto-optimal objects by local criteria, parametric synthesis of their scalar evaluation model, calculation of their generalized evaluations and their ordering [17 - 18].

At the first stages of formalization the essence of the problem of choosing the best user object can be represented by a logical statement «it is necessary to find o^o " or formally $< -, o^o >$ (where $o^o \in O$ is the best user object from the set of considered ones). At that, the situation of choosing the best object d is usually not clearly defined (formally $< d, - >$). To proceed to the choice problem $< d, o^o >$, let us decompose the problem into a set of problems of the form: "given $< d, - >$, necessary $< d, o^o >$" or "given $< -, o^o >$, necessary $< d, o^o >$", i.e.:

$$<< d, - >, < d, o^o >>, \quad << -, o^o >, < d, o^o >>. \quad (4)$$

The main tasks in the development of recommendation systems obtained as a result of decomposition of the decision-making problem (4) are: $Task_1$ - allocation of the set of admissible objects $O = \{o_i\}$, $i = \overline{1,n}$ satisfying the set of restrictions on the set of local criteria $k_l(o_i)$, $l = \overline{1,p}$; $Task_2$ – allocation of a subset of effective (Pareto-optimal) objects on the set of local criteria $O^E \subseteq O$; $Task_3$ – ranking of objects $o_i \in O^E$.

It is known that in practice a significant part among the objects of multicriteria choice $O = \{o_i\}$, $i = \overline{1,n}$, the information about which is in the system, can be dominated [17 - 18]. Relative to them there are objects best simultaneously on all quality indicators $k_l(o_i)$, $l = \overline{1,p}$.

An object of choice $o^E \in O$ belongs to a subset of non-dominated (Pareto-optimal, efficient) $O^E \subseteq O$ if there is no object for which the inequalities are fulfilled:

$$k_l(o_i) \geq k_l(o^E), \text{ if } k_l(o_i) \to max, \; l = \overline{1,p}, \quad (5)$$

$$k_l(o_i) \leq k_l(o^E), \text{ if } k_l(o_i) \to min, \; l = \overline{1,p} \quad (6)$$

and at least one of them was strict.

The results of experimental studies for uniform distribution of object characteristics in the space of local criteria $k_l(o_i)$, $l = \overline{2,7}$ showed that: the powers of Pareto-optimal object subsets $|O^E|$ depending on the number of local criteria p and the powers of the sets of admissible objects $|O|$ have a stable tendency to growth, and the relative sizes of Pareto-optimal object subsets $|O^E| / |O|$ have a stable tendency to reduction (table 1, fig. 2).

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

Table 1. *Relative power of a subset of Pareto-optimal objects*

p	Number of objects of choice, *n*									
	10	20	30	40	50	60	70	80	90	100
2	0,200	0,150	0,133	0,100	0,100	0,083	0,071	0,075	0,078	0,080
3	0,400	0,300	0,233	0,225	0,160	0,150	0,286	0,275	0,278	0,260
4	0,600	0,450	0,400	0,350	0,240	0,317	0,400	0,350	0,300	0,280
5	0,700	0,600	0,500	0,650	0,580	0,567	0,500	0,475	0,422	0,430
6	0,900	0,750	0,767	0,725	0,700	0,683	0,600	0,575	0,656	0,630
7	1,000	0,900	0,933	0,900	0,840	0,783	0,729	0,713	0,722	0,710

On this basis, using the method of even comparisons, a preliminary separation of a subset of non-dominated objects of choice is proposed [17]. To further reduce the set of non-dominant objects and to compose them, it is proposed to use the idea of the combined method [18].

Its use implies that each object of choice $o_i \in O^E$ is assigned a scalar estimate of its generalized utility, reflecting its value for the user $P(o_i)$:

$$o_i \succ o_j \leftrightarrow P(o_i) > P(o_j)\,, \qquad (7)$$

the value of which will determine the ordering of the whole set of objects: $o_i \succ o_j \succ \ldots \succ o_z$, $o_i, o_j, \ldots, o_z \in O' \subseteq O$.

For quantitative scalar estimation of generalized utility of objects the classical additive convolution of local criteria can be used [17 - 18]:

$$P(o_i) = \sum_{l=1}^{p} \lambda_l \xi_l(o_i)\,, \qquad (8)$$

$$\xi_l(o_i) = [(k_l(o_i) - k_l^-)/(k_l^+ - k_l^-)]^{\mu_l}\,,\ l = \overline{1,p}\,, \qquad (9)$$

where λ_l, $l = \overline{1,p}$ – parameters that characterize the importance of the individual properties of the object of choice $k_l(o_i)$, $\lambda_l \geq 0$, $\sum_{l=1}^{p} \lambda_l = 1$ for the user; $\xi_l(o_i)$ – value of the utility function of the local criterion value $k_l(o_i)$; k_l^+, k_l^-, $l = \overline{1,p}$ – best and worst values of the l-th local criterion; μ_l – parameter determining the type of dependence (9): linear, convex or concave.

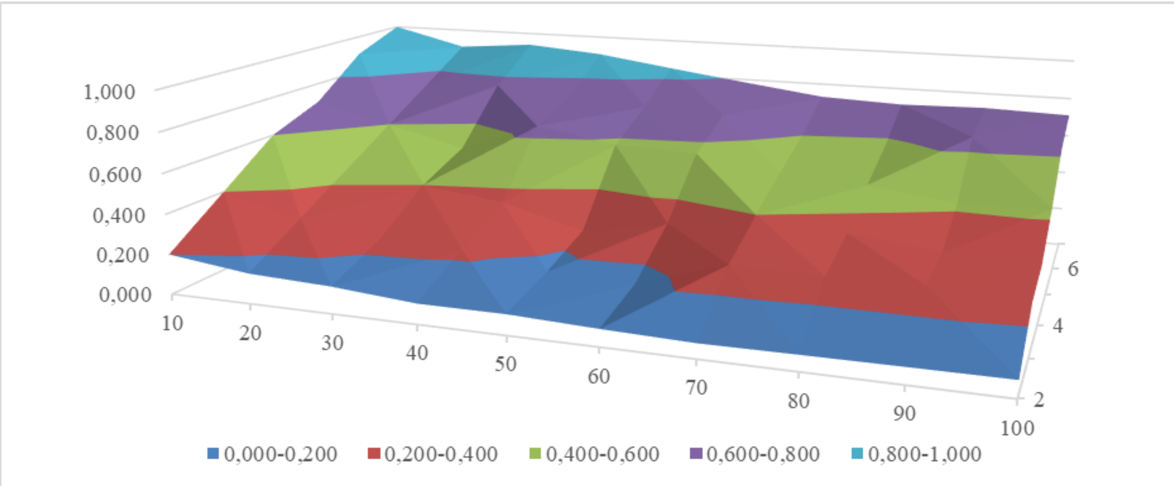


Fig. 2. Relative power of a subset of Pareto-optimal objects

The user of the system by the results of the analysis of proposals among the Pareto-optimal objects on the set of local criteria $k_l(o_i)$, $l = \overline{1,p}$ determines its advantages. In the easiest case, he chooses the best object $o^o \in O^E$ in his opinion. This choice corresponds to the binary relation of the strict advantage of this kind:

$$R(O^E) = \{< o^o, o_i >:\ o^o, o_i \in O^E,\ o^o \succ o_i\}. \qquad (10)$$

In general, using quantitative or qualitative estimates, the user can set the order among the non-dominant objects offered to him:

$$o_i \succ o_j \succ \ldots \succ o_z,\ o_i, o_j, \ldots, o_z \in O^E. \qquad (11)$$

or determine the advantages among the pairs of objects offered for comparison:

$$R(O^E) = \{< o_i, o_j >:\ o_i, o_j \in O^E,\ o_i \succ o_j\}. \qquad (12)$$

On the basis of the established relation of strict advantage (10), (11) or (12) let us make a system of inequalities of the form:

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$P(o_i,\lambda) > P(o_j,\lambda),\ \langle o_i,o_j\rangle \in R(O^E),\ \sum_{l=1}^{p}\lambda_l = 1,\ \lambda_l \ge 0,\ (13)$$

where $\lambda = [\lambda_1, \lambda_2, ..., \lambda_p]$ – vector of model weighting coefficients (8).

The problem of parametric synthesis of the model (8) consists in determining the coordinates of the vector $\lambda = [\lambda_l]_{l=1}^{p}$ corresponding to the established system of inequalities (13), as well as the condition of its normalization.

If the user preferences (10), (11) or (12) are non-contradictory, the system (13) can have many solutions. To regularize the problem, it is proposed to reduce the process of its solution to the search for its Chebyshev point [17 - 18]. In this case, if the user-defined binary relation (10), (11) or (12) is consistent, the system of inequalities (13) will be compatible. Then the resulting set of model parameters $\lambda = [\lambda_1, \lambda_2, ..., \lambda_p]$ (8) will be as stable as possible to probable changes in user preferences.

Using the set parameter $\lambda = [\lambda_1, \lambda_2, ..., \lambda_p]$ values, let's calculate the value of the generalized value function (8) of the proposed user objects of the recommender system $P(o_i)$, $o_i \in O^E$. On the basis of obtained values of parameters $\lambda = [\lambda_1, \lambda_2, ..., \lambda_p]$ and properties of objects set by values of local criteria $k_l(o_i)$, $l = \overline{1,p}$ the correct orders will be formed when changing a set of objects of choice for the user of the system $O = \{o_i\}$, $i = \overline{1,n}$.

Let us consider the problem of putting in order 8 objects of the recommender system by solving the problem using the general utility model (8). Each of the objects is estimated by four local criteria $k_l(o_i) \to max$, $l = \overline{1,4}$ on a ten-point scale. Let's calculate by relation (9) the value of utility functions of local criteria $\xi_l(o_i)$, $l = \overline{1,4}$ for $\mu_l = 1$ (table 2).

Table 2. *Characteristics of user choice objects*

o_i	$k_1(o_i)$	$k_2(o_i)$	$k_3(o_i)$	$k_4(o_i)$	$\xi_1(o_i)$	$\xi_2(o_i)$	$\xi_3(o_i)$	$\xi_4(o_i)$	$P(o_i)$
o_1	8,51	9,74	5,95	9,78	0,851	0,974	0,595	0,978	0,8692
o_2	9,26	7,07	7,91	9,43	0,926	0,707	0,791	0,943	0,8346
o_3	9,72	8,86	8,45	5,93	0,972	0,886	0,845	0,593	0,8296
o_4	9,58	7,01	7,87	8,78	0,958	0,701	0,787	0,878	0,8244
o_5	6,51	8,62	7,89	9,65	0,651	0,862	0,789	0,965	0,8193
o_6	7,99	9,15	9,02	4,35	0,799	0,915	0,902	0,435	0,7692
o_7	4,58	8,34	9,75	8,17	0,458	0,834	0,975	0,817	0,7639
o_8	9,84	5,25	3,51	8,15	0,984	0,525	0,351	0,815	0,6743
o_9	5,19	8,38	6,95	4,97	0,519	0,838	0,695	0,497	0,6488
o_{10}	8,92	0,62	8,19	8,51	0,892	0,062	0,819	0,851	0,6072
o_{11}	9,81	7,67	2,75	2,16	0,981	0,767	0,275	0,216	0,5919
o_{12}	9,89	3,45	3,06	6,32	0,989	0,345	0,306	0,632	0,5666

Let the user, based on his preferences, determine the order of the form (11) on a given set of objects:

$$o_1 \succ o_2 \succ o_3 \succ o_4 \succ o_5 \succ o_6 \succ o_7 \succ o_8 . \qquad (14)$$

To solve the problem of parametric synthesis of the general utility model (8) by the method of comparator identification, let us make a system of inequalities and equations (13) and reduce the process of its solution to the search for its Chebyshev point:

$$\begin{cases} \eta_j(\lambda) \equiv \sum_{l=1}^{4}\lambda_l\,\xi_l(o_i) - \sum_{l=1}^{4}\lambda_l\,\xi_l(o_j) > 0, \langle o_i,o_j\rangle \in R(O^E),\ j = \overline{1,7}, \\ \eta_8(\lambda) \equiv \sum_{l=1}^{4}\lambda_i = 1,\ \lambda_l \ge 0,\ l = \overline{1,4}. \end{cases} \qquad (15)$$

Stable estimates of the vector of model parameters $\lambda = [\lambda_1, \lambda_2, \lambda_3, \lambda_4]$ (8) is a solution of the problem of searching the Chebyshev point [17 - 18]:

$$\begin{cases} \eta_j(\lambda) + \lambda_5 > 0, \quad j = \overline{1,7}, \\ \eta_8(\lambda) \equiv \sum_{l=1}^{4}\lambda_l = 1, \quad \lambda_l \ge 0, \quad l = \overline{1,4}, \\ \lambda_5 \to min. \end{cases} \qquad (16)$$

The solution of problem (16) will be a vector of weight coefficients of local criteria. $\lambda = [0{,}250;\ 0{,}314;\ 0{,}198;\ 0{,}238]$. The values of the generalized value function (8) of the objects $P(o_i)$, $i = \overline{1,8}$ calculated on their basis fully correspond to the user's preferences (14). Using the obtained values of weighting coefficients, the estimates $P(o_i)$ of new

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

objects $i=\overline{9,12}$ added to the system are calculated. On the basis of the expanded table on the basis of the necessary number of objects in the list and values of the function of the generalized value, the new list of recommendations is formed (tab. 2).

According to the results of experiments, it was found that the proposed method of order formation based on comparator identification technology has lower temporal complexity when including new objects in the system than the method of collaborative filtering.

For more adequate identification of the user benefits of the recommender system, if sufficient computational resources are available, an additive-multiplicative model based on the Kolmogorov-Gabor polynomial can be used [17 - 18]:

$$P(o_i)=\sum_{j=1}^{p}\lambda_l\xi_l(o_i)+\sum_{j=1}^{p}\sum_{k=j}^{p}\lambda_{jk}\xi_j(o_i)\xi_k(o_i)+\sum_{j=1}^{p}\sum_{k=j}^{p}\sum_{l=k}^{p}\lambda_{jkl}\xi_j(o_i)\xi_k(o_i)\xi_l(o_i)+\dots \quad (14)$$

where λ_j, λ_{jk}, λ_{jkl} – weighting coefficients assessing the mutual importance of local criteria $k_i(o_i)$, $k_j(o_i)$, $k_l(o_i)$ and their products; $0<\xi_j(o_i)<1$, $j=\overline{1,p}$ – value of the utility function of the local criterion $k_j(o_i)$, $j=\overline{1,p}$ for an object from the set of non-dominant $o_i\in O^E$.

Model (14) is universal and allows to describe all possible advantages of the system users. Its special case under $\lambda_{jk}=0$, $\lambda_{jkl}=0$, $j,k,l=\overline{1,p}$ is the classical additive model of scalar multicriteria estimation (8). In addition, the accuracy of determining user benefits of recommender systems based on models (8) and (14) can be improved by using universal utility functions that allow to realize both linear and nonlinear (including S- and Z-shaped) dependences on the values of local criteria [20 - 22].

The proposed method allows to take into account the set of object characteristics defined by the values of local criteria, has a lower time complexity than the method of collaborative filtering, allows to take into account the advantages of users of recommender systems more accurately, provide recommendations only to those objects that belong to the Pareto-optimal set and on this basis improve the quality of orders of proposals formed for them.

Conclusions

According to the results of the review of the current state of the problem of determining benefits in recommender systems, it was found that they use information about the similarity of the characteristics of objects or the acts of selection of objects by users with similar preferences to form suggestions. Existing methods for providing recommendations based on content, collaborative filtering, and knowledge use only generalized evaluations of objects and have relatively high temporal complexity. At the same time, it is known that a significant number among the objects that make it to the recommendation lists may be inefficient under Pareto. Proceeding from the fact that recommendation systems are essentially specific decision support systems, models and methods of the theory of multicriteria decision making are used to improve their efficiency.

To improve the quality of recommendations, it was proposed to use the evaluation of objects by the set of indicators, which will be considered as local criteria of their effectiveness and to carry out a preliminary filtering of objects included in the lists by checking them for Pareto-optimality. For the inclusion of objects in the lists of recommended, it turned out to be expedient to perform their scalar multicriteria evaluation with the use of generalized value functions. Depending on amount of data, available computational and time resources, both classical additive model and universal additive-multiplicative model based on Kolmogorov-Gabor polynomial can be used for this purpose. For the structural-parametric synthesis of the model, it is proposed to use the comparator identification technology, which allows to solve the problem using both active experiments and collection of information about the facts of users' choices.

The developed method of benefits establishment extends the methodological foundations of automation of development and operation of recommender systems, other multicriteria decision support systems, allows to carry out correct reduction of the set of non-dominant objects for the final choice taking into account the knowledge and experience of users, which are difficult to formalize. Practical use of the received results at the expense of more economical method of formation of lists at addition of new objects will allow to lower time and capacitive complexity of procedures of granting of recommendations, and at the expense of consideration of set of weighted local indicators and allocation of set of non-dominant objects – to raise quality of the given recommendations.

References

1. Wang, Wei (2018), "Recommended System of Application and Development", *AIP Conference Proceedings 1955, 040180.* **DOI:** https://doi.org/10.1063/1.5033844
2. Isinkaye, F. O., Folajimi, Y. O., Ojokoh, B. A. (2015), "Recommendation systems: Principles, methods and evaluation", *Egyptian Informatics Journal,* Vol. 16, Issue. 3, P. 261–273. **DOI:** https://doi.org/10.1016/j.eij.2015.06.005
3. Veres, O., Levus, Ya. (2022), "Recommendation system for leisure planning in quarantine conditions" ["Rekomendacijna systema planuvannya dozvillya v umovax karantynu"], *Bulletin of the Lviv Polytechnic National University. Information systems and networks,* Vol. 11, P. 127–144. **DOI:** https://doi.org/10.23939/sisn2022.11.127

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

4. Lobur, M. V., Shwarz, M. Ye., Steh Yu. V. (2018), "Models and methods of forecasting recommendations in collaborative recommender systems" ["Modeli i metody prognozuvannya rekomendacij v kolaboratyvnyx rekomendacijnyx systemax"], *Bulletin of the Lviv Polytechnic National University, Information systems and networks,* No. 901, P. 68–75.
5. Chalyi, S., Leshchynskyi, V., Leshchynska, I. (2019), "Addition of input data of the recommender system in the situation of a cyclical cold start using temporal restrictions of the type "next" ["Dopovnennya vxidnyx danyx rekomendacijnoyi systemy v sytuaciyi cyklichnogo xolodnogo startu z vykorystannyam temporalnyx obmezhen typu "next""], *Control, navigation and communication systems,* Vol. 4 (56), P. 105–109. **DOI:** https://doi.org/10.26906/SUNZ.2019.4.105
6. Velasquez, Mark, Hester, Patrick T. (2013), "An Analysis of Multi-Criteria Decision Making Methods", *International Journal of Operations Research*, Vol. 10, No. 2, P. 56–66.
7. Zlaugotne, B., Zihare, L., Balode, L., Kalnbalkite, A., Khabdullin, A., Blumberga, D. (2020), "Multi-Criteria Decision Analysis Methods Comparison", *Environmental and Climate Technologies*, 24 (1), P. 454–471. **DOI:** https://doi.org/10.2478/rtuect-2020-0028
8. Mark Velasquez1 and Patrick T. Hester (2013),"An Analysis of Multi-Criteria Decision Making Methods", *International Journal of Operations Research*, Vol. 10, No. 2, P. 56–66.
9. Ishizaka, A., Nemery, P. (2013), *Multi-Criteria Decision Analysis*, John Wiley & Sons, 312 p.
10. Bernasconi, M., Choirat, C., & Seri, R. (2014), "Empirical properties of group preference aggregation methods employed in AHP: Theory and evidence", *European Journal of Operational Research*, Vol. 232, Issue. 3, P. 584–592. **DOI:** https://doi.org/10.1016/j.ejor.2013.06.014
11. Ataei, M., Shahsavany, H., & Mikaeil, R. (2013), "Monte Carlo Analytic Hierarchy Process (MAHP) approach to selection of optimum mining method", *International Journal of Mining Science and Technology*, 23, P. 573–578. **DOI:** https://doi.org/10.1016/j.ijmst.2013.07.017
12. Bagočius, V., Zavadskas, E. K., & Turskis, Z. (2014), "Multi-person selection of the best wind tur-bine based on the multi-criteria integrated additive-multiplicative utility function", *Journal of Civil Engineering and Management*, 20, P. 590–599. **DOI:** 10.3846/13923730.2014.932836
13. Baky, I. A. (2014), "Interactive TOPSIS algorithms for solving multi-level non-linear multi-objective decision-making problems", *Applied Mathematical Modelling*, 38, P. 1417–1433. **DOI:** https://doi.org/10.1016/j.apm.2013.08.016
14. Baky, I. & Abo-Sinna, M. (2013), "TOPSIS for bi-level MODM problems", *Applied Mathematical Modelling,* 37 (3), P. 1004–1015. **DOI:** https://doi.org/10.1016/j.apm.2012.03.002
15. Ekstrand, M. D., Riedl, J. T., Konstan, J. A. (2011), "Collaborative Filtering Recommender Systems", *Foundations and Trends in Human–Computer Interaction*, Vol. 4, No. 2, P. 81–173. **DOI:** http://dx.doi.org/10.1561/1100000009
16. Son Le Hoang (2016), "Dealing with the new user cold-start problem in recommender systems: A comparative review", *Information Systems*, 58, P. 87–104. **DOI:** https://doi.org/10.1016/j.is.2014.10.001
17. Beskorovainyi, V. V., Petryshyn, L. B., Shevchenko, O. Y. (2020), "Specific subset effective option in technology design decisions", *Applied Aspects of Information Technology*, Vol. 3, No.1, P. 443–455. **DOI:** https://doi.org/10.15276/aait.01.2020.6
18. Beskorovainyi, V. (2020), "Combined method of ranking options in project decision support systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (14), P. 13–20. **DOI:** https://doi.org/10.30837/ITSSI.2020.14.013
19. Ricci, F., Rokach, L., Shapira, B., Kantor, P. B. (2001), *Recommender Systems Handbook*, New York: Springer, 845 p.
20. Beskorovainyi, V., Berezovskyi, G. (2017), "Estimating the properties of technological systems based on fuzzy sets", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (1), P. 14–20.
21. Beskorovainyi, V., Berezovskyi, H. (2017), "Identification of preferences in decision support systems", *ECONTECHMOD*, Vol. 06, No. 4, P. 15–20.
22. Beskorovainyi, V. (2017), "Parametric synthesis of models for multi criterial estimation of technological systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (2), P. 5–11.

Received 27.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Безкоровайний Володимир Валентинович – доктор технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри системотехніки, Харків, Україна; e-mail: vladimir.beskorovainyi@nure.ua; ORCID: https://orcid.org/0000-0001-7930-3984.

Бескоровайный Владимир Валентинович – доктор технических наук, профессор, Харьковский национальный университет радиоэлектроники, профессор кафедры системотехники, Харьков, Украина.

Beskorovainyi Vladimir – Doctor of Sciences (Engineering), Professor, Kharkiv National University of Radio Electronics, Professor of the Department of System Engineering, Kharkiv, Ukraine.

Колесник Людмила Володимирівна – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри системотехніки, Харків, Україна; e-mail: liudmyla.kolesnyk@nure.ua; ORCID: https://orcid.org/0000-0003-4417-7759.

Колесник Людмила Владимировна – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры системотехники, Харьков, Украина.

Kolesnyk Lyudmyla – Candidate of Technical Sciences, Associate Professor, Kharkiv National University of Radio Electronics, Professor of the Department of System Engineering, Kharkiv, Ukraine.

Альохіна Марія Михайлівна – магістр комп'ютерних наук, Харківський національний університет радіоелектроніки, Харків, Україна; e-mail: mariia.alokhina@nure.ua; ORCID: https://orcid.org/0000-0001-7346-6096.

Алёхина Мария Михайловна – магистр компьютерных наук, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

Alokhina Mariia – Master of Computer Science, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

Косенко Віктор Васильович – доктор технічних наук, професор, Національний університет «Полтавська політехніка імені Юрія Кондратюка», професор кафедри автоматики, електроніки та телекомунікацій, Полтава, Україна; kosvict@gmail.com; ORCID ID – http://orcid.org/0000-0002-4905-8508.

Косенко Виктор Васильевич – доктор технических наук, профессор, Национальный университет «Полтавская политехника имени Юрия Кондратюка», профессор кафедры автоматики, электроники и телекоммуникаций, Полтава, Украина.

Viktor Kosenko – Doctor of Sciences (Engineering), Professor of Automation, Electronic and Telecommunication Department of National University «Yuri Kondratyuk Poltava Polytechnic, Poltava, Ukraine.

ВИЗНАЧЕННЯ ПЕРЕВАГ У РЕКОМЕНДАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ТЕХНОЛОГІЇ КОМПАРАТОРНОЇ ІДЕНТИФІКАЦІЇ

Предметом дослідження в статті є процес ранжування об'єктів у списках рекомендаційних систем. **Мета** роботи – підвищення ефективності рекомендаційних систем за рахунок удосконалення методу визначення переваг між об'єктами у списках з використанням теорії прийняття багатокритеріальних рішень. У статті вирішуються наступні **завдання:** огляд і аналіз сучасного стану проблеми встановлення переваг між об'єктами та їхнього ранжування у списках рекомендаційних систем; аналіз методів фільтрації, що використовуються в рекомендаційних системах; декомпозиція проблеми підтримки прийняття рішень з вибору об'єктів; розробка комбінованого методу ранжування об'єктів у списках рекомендаційних систем, який об'єднує процедури виділення підмножини Парето-оптимальних об'єктів, структурно-параметричного синтезу моделі скалярного багатокритеріального оцінювання та оцінювання всієї множини виділених об'єктів. Використовуються такі **методи:** математичного моделювання, теорії систем, теорії корисності, теорії прийняття рішень, оптимізації та дослідження операцій. **Результати.** За результатами аналізу сучасної методології ранжування об'єктів у списках рекомендаційних систем встановлена можливість підвищення їхньої ефективності. Для врахуванням факторів, що важко піддаються формалізації, знань і досвіду користувачів запропоновано реалізувати визначення переваг між об'єктами з використанням теорії прийняття багатокритеріальних рішень. Виконана декомпозиція проблеми формування списків рекомендаційних систем на задачі виділення підмножини Парето-оптимальних об'єктів, структурно-параметричного синтезу моделі скалярного багатокритеріального оцінювання та оцінювання множини виділених об'єктів. Розроблено комбінований метод ранжування варіантів, який об'єднує процедури технологій ординалістичного та кардиналістичного впорядкування та дозволяє коректно скорочувати підмножин об'єктів, що включаються до списків рекомендацій. **Висновки.** Розроблений метод встановлення переваг розширює методологічні засади автоматизації процесів розробки та експлуатації рекомендаційних систем, інших систем підтримки прийняття багатокритеріальних рішень, дозволяє здійснювати коректне скорочення множини недомінованих об'єктів для остаточного вибору з урахуванням факторів, що важко піддаються формалізації, знань і досвіду користувачів. Практичне використання отриманих результатів за рахунок більш економного методу формування списків при додаванні нових об'єктів дозволить знизити часову й ємнісну складності процедур надання рекомендацій, а за рахунок врахування множини зважених локальних показників і виділення множини недомінованих об'єктів – підвищити якість рекомендацій, що надаються.

Ключові слова: багатокритеріальне оцінювання; компараторна ідентифікація; рекомендаційна система; ранжування об'єктів; структурно-параметричний синтез.

ОПРЕДЕЛЕНИЕ ПРЕДПОЧТЕНИЙ В РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ НА ОСНОВЕ ТЕХНОЛОГИИ КОМПАРАТОРНОЙ ИДЕНТИФИКАЦИИ

Предметом исследования в статье является процесс ранжирования объектов в списках рекомендательных систем. **Цель** работы – повышение эффективности рекомендательных систем за счет усовершенствования метода определения предпочтений между объектами в списках с использованием теории принятия многокритериальных решений. В статье решаются следующие **задачи:** обзор и анализ современного состояния проблемы определения предпочтений между объектами и их ранжирование в списках рекомендательных систем; анализ методов фильтрации, используемых в рекомендательных системах; декомпозиция проблемы поддержки принятия решений по выбору объектов; разработка комбинированного метода ранжирования объектов в списках рекомендательных систем, объединяющего процедуры выделения подмножества Парето-оптимальных объектов, структурно-параметрического синтеза модели скалярного многокритериального оценивания и оценки всего множества выделенных объектов. Используются следующие **методы:** математического моделирования, теории систем, теории полезности, теории принятия решений, оптимизации и исследования операций. **Результаты.** По результатам анализа современной методологии ранжирования объектов в списках рекомендательных систем установлена возможность повышения их эффективности. Для учета трудно поддающихся формализации факторов, знаний и опыта пользователей предложено реализовать определение предпочтений между объектами с использованием теории принятия многокритериальных решений. Выполнена декомпозиция проблемы формирования списков рекомендательных систем на задачи выделения подмножества Парето-оптимальных объектов, структурно-параметрического синтеза модели скалярного многокритериального оценивания и оценки множества выделенных объектов. Разработан комбинированный метод ранжирования вариантов, объединяющий процедуры технологий ординалистического и кардиналистического упорядочения и позволяющий корректно сокращать подмножества объектов, включаемых в списки рекомендаций. Разработанный метод определения предпочтений расширяет методологические основы автоматизации процессов разработки и эксплуатации рекомендательных систем, других систем поддержки принятия многокритериальных решений, позволяет **Выводы.** осуществлять корректное сокращение множества недоминированных объектов для окончательного выбора с учетом трудно поддающихся формализации факторов, знаний и опыта пользователей. Практическое использование полученных результатов за счет более экономного метода формирования списков при добавлении новых объектов позволит снизить временную и емкостную сложности процедур предоставления рекомендаций, а за счет учета множества взвешенных локальных показателей и выделения множества недоминированных объектов – повысить качество предоставляемых рекомендаций.

многокритериальное оценивание; компараторная идентификация; рекомендательная система; ранжирование объектов **Ключевые слова:**; структурно-параметрический синтез.

Бібліографічні описи / Bibliographic descriptions

Безкоровайний В. В., Колесник Л. В., Альохіна М. М., Косенко В. В. Визначення переваг у рекомендаційних системах на основі технології компараторної ідентифікації. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 14–21. DOI: https://doi.org/10.30837/ITSSI.2022.20.014

Beskorovainyi, V., Kolesnyk, L., Alokhina, M., Kosenko, V. (2022), "Determining preferences in recommender systems based on comparator identification technology", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 14–21. DOI: https://doi.org/10.30837/ITSSI.2022.20.014

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 621.3.01+621.38 DOI: https://doi.org/10.30837/ITSSI.2022.20.022

P. Klimushyn, T. Solianyk, O. Mozhaiev, Y. Gnusov, O. Manzhai, V. Svitlychny

CRYPTO-RESISTANT METHODS AND RANDOM NUMBER GENERATORS IN INTERNET OF THINGS (IOT) DEVICES

Subject of research: crypto-resistant methods and tools of generating random sequences and hardware support of cryptographic transformations in IoT devices. The **aim** of the article is to study crypto-resistant methods and tools for generating and testing random sequences suitable for use in IoT devices with limited resources; determination of circuit implementations of random sequences hardware generators; formation of conclusions on the use of random number generators (RNG) in cryptographic protection systems of the IoT network. The article solves the following **tasks:** analysis of methods and hardware for generating random sequences to protect IoT solutions with limited resources; identification of safe and effective technologies for the implementation of RNG; classification of RNG attacks; analysis of the shortcomings of the practical use of statistical test packages to assess the quality of random sequences of RNG; evaluation of the speed of cryptoaccelerators of hardware support for cryptographic transformations; providing practical guidance on RNG for use in resource-constrained IoT devices. Research **methods:** method of structural and functional analysis of RNG and IoT devices, cryptographic methods of information protection, methods of random sequence generation, method of stability analysis of systems, methods of construction of autonomous Boolean networks and Boolean chaos analysis, methods of quality assessment of random sequences. **Results** of work: the analysis of technologies and circuit decisions of hardware RNG on characteristics: quality of numbers' randomness and unpredictability of sequences, speed, power consumption, miniaturization, possibility of integral execution; providing practical recommendations for the use of RNG in cryptographic protection systems of the IoT network. The **novelty** of the study is the analysis of methods and hardware to support technologies for generating random sequences in the system of cryptographic protection of IoT solutions; classification of attacks on RNG and features of protection against them; identification of effective RNG technologies and circuit solutions for use in low-power IoT devices with limited computing resources; providing practical recommendations for the use of RNG in cryptographic protection systems of the IoT network. The analysis of technologies and circuit solutions allowed to draw the following **conclusions:** protection of IoT solutions includes: security of IoT network nodes and their connection to the cloud using secure protocols, ensuring confidentiality, authenticity and integrity of IoT data by cryptographic methods, attack analysis and network cryptographic stability; the initial basis for the protection of IoT solutions is the true randomness of the formed RNG sequences and used in algorithms for cryptographic transformation of information to protect it; feature of IoT devices is their heterogeneity and geographical distribution, limited computing resources and power supply, small size; The most effective (reduce power consumption and increase the generation rate) for use in IoT devices are RNG exclusively on a digital basis, which implements a three-stage process: the initial digital circuit, normalizer and random number flow generator; Autonomous Boolean networks (ABN) allow to create RNG with unique characteristics: the received numbers are really random, high speed – the number can be received in one measure, the minimum power consumption, miniature, high (up to 3 GHz) throughput of Boolean chaos; a promising area of ABN development is the use of optical logic valves for the construction of optical ABN with a bandwidth of up to 14 GHz; the classification of known classes of RNG attacks includes: direct cryptanalytic attacks, attacks based on input data, attacks based on the disclosure of the internal state of RNG, correlation attacks and special attacks; statistical test packages to evaluate RNG sequences have some limitations or shortcomings and do not replace cryptanalysis; Comparison of cryptoaccelerators with cryptographic transformation software shows their significant advantages: for AES block encryption algorithm, speeds increase by 10-20 times in 8/16-bit cryptoaccelerators and 150 times in 32-bit, growth hashing of SHA-256 in 32-bit cryptoaccelerators more than 100 times, and for the NMAS algorithm - up to 500 times.

Keywords: Internet of Things; random number generator; cryptocurrency; cryptanalysis; cryptographic keys; encryption; hashing; Autonomous Boolean Networks; Boolean chaos; statistical tests; cryptoaccelerators.

Introduction

The Internet of Things (IoT) is a major IT development trend that contributes to societal development in the areas of human life services, public safety, medical services, industrial process management, transportation, competitiveness and business productivity. The interconnection of IoT nodes connected to the network negatively affects the overall level of security and crypto-resistance of the system. This problem is exacerbated by factors of mass, heterogeneity in the structure of the devices involved, limited computing and energy resources, the automation of connecting IoT nodes to the network, gullibility from the users and protection of their personal data and privacy. Problems of security are a major restraining factor in the use of IoT technologies.

Protecting IoT solutions includes securing IoT network nodes and their connection to the cloud using secure protocols, confidentiality, authenticity and integrity of data during transmission, processing and storage on the IoT network, as well as resistance to physical and virtual attacks. Main properties of information (confidentiality, authenticity and integrity) are preserved by cryptographic methods, such as data encryption and data hashing using cryptographic keys.

High-performance information systems are manufactured on general-purpose microprocessors with significant processing power, large memory capacity and power-intensive supply. Along with this, for embedded IoT systems the computing power, power consumption, size and price are limited. There is a problem of implementation of widespread cryptographic algorithms (AES, SHA, HMAC, RSA, DH, ECC, etc.) in embedded IoT devices.

In turn, the generation of cryptographic keys is based on the unpredictability of random sequences of numbers generated by LFO. That is, the initial basis for the protection of IoT solutions is the true randomness of LFO number sequences. Therefore, the problem of information protection in IoT devices is related to the simultaneous

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

optimization of the level of security of HFSCs, their productivity and price under the above-mentioned constraints. In addition, a characteristic of IoT devices is their heterogeneity and geographical distribution. Consequently, the generation of random sequences by software using a deterministic algorithm in high-performance microprocessor systems does not ensure the proper quality of these sequences. Such sequences are pseudorandom, which means that the possibility of their predictability grows, and, as a result, the crypto resistance of the systems decreases.

To overcome the above-mentioned problems, a wide range of technical solutions for generating truly random sequences using hardware HFOs using physical sources of unexpected noise, including quantum processes or Boolean chaos in digital circuits is implemented. Specialized hardware components (cryptoaccelerators) are created in general-purpose microcontrollers of different families, significantly accelerating random sequence generation and execution of existing cryptoalgorithms. Such specialized modules are effective for securing IoT solutions and are a critical trend in IoT deployments in resource-constrained environments.

Analysis of the literature. Analysis of scientific and technical literature shows that in recent decades a large number of elementary pseudorandom number generators, which include linear congruent generators, Fibonacci generators with delay [1], was developed and investigated. Many years of research led to the conclusion that all of them are not crypto-resistant and can be part of the shapers of pseudorandom sequences. The most successful such generators in terms of cryptography are considered in detail in the work of Bruce Schneier [2]. Over time, algorithms that seemed previously reliable find new weaknesses. For this reason, in the process of development of cryptographic protocols there is a question of finding new engineering solutions to build effective crypto-resistant generators, free of the identified weaknesses.

In contrast to other engineering problems, the development of a new random number generation algorithm is different in that a reliable answer to the question about the effectiveness of the found solution may appear some time later, when an individual cryptanalysis method is developed for it. The developer can be satisfied only with results of preliminary testing of the solution by existing test packages [3-5].

The crypto resistance of generators is a key factor for the whole system of information protection by means of cryptographic transformations. The impact of this factor on the cryptocurrency of the protection system is studied in a large number of works, in particular [6, 7], etc.

The best choice for forming truly random sequences is hardware implementation of generators. These include generators using physical processes in electronic elements [8, 9], quantum generators [10-12], digital generators based on autonomous Boolean networks [13-16]. A general trend in the development of hardware generators is the creation of specialized modules in integral design [9]. Implementation of such modules is effective for low-power IoT devices.

Thus, the analysis of scientific sources showed a huge range of means of generating random sequences. IoT network security requires crypto-resistant, low-power, miniaturized RNGs.

The **purpose** of this article is to study crypto-resistant methods and means of generating and testing random sequences suitable for IoT devices with limited resources; definition of schematic implementations of the hardware random sequence generators; formation of conclusions for the use of RNG in cryptographic network protection systems of IoT devices.

1. Crypto-resistant methods of random number generation

Random number sequences are used for:

- generation of session, public and secret cryptographic keys in symmetric and asymmetric encryption systems, electronic signature systems;
- random data sets in IoT identification and authentication protocols.

The quality of cryptographic key formation and random datasets determines the cryptographic stability of the entire IoT network as a whole.

Methods of generating keys and cryptographic data are divided into two classes: random (based on physical processes using hardware) and pseudorandom (based on software, mathematical software). The tools that generate pseudorandom number sequences are called pseudorandom number generators (PRNG) [17].

In hardware RNG, each bit of raw data is based on an unanticipated physical process, that is, it is produced from the noise signal of the internal source of physical analog noise. The value of a random number obtained directly by discretizing the analog noise signal.

PRNGs are implemented programmatically according to the algorithm, starting from an initial value that can be generated by a hardware entropy source. Due to the deterministic nature of the processing, it is assumed that PRNGs produce pseudorandom, not random bits. The initial number used to implement PRNG must contain sufficient entropy to guarantee randomness [18]. For them, the generation of new random numbers does not increase the entropy of the initial number.

Nowadays RNG based on different physical processes, such as electric current noise in electric elements (resistors, diodes, transistors), radioactive decay, atmospheric turbulence, cosmic radiation, photoelectric effect, quantum phenomena have been developed.

Disadvantage of the most typical random number generators based on physical processes is the emergence in the process of generation of so-called shifted sequences (in such sequences a certain combination of numbers or bits is most often repeated). Offset occurs because of the difficulty in designing and implementing precisely balanced physical schemes of number generation. To

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

remove such a disadvantage there are algorithms for further processing.

2. Effective technologies for implementing hardware random number generators

Modern RNG in IoT devices are based on physical principles and implemented on electronic components. They use, for example, such physical processes as thermal noise in electronic elements or avalanche breakdown of p-n junction with reverse bias in Zenner diode [8]. The disadvantage of such generators is the need to manufacture a special analog circuit, which greatly complicates the manufacture of integrated circuits and makes it impossible to implement in a programmable logic integrated circuit (PLIC).

In addition, RNG are known which use the difference in frequency of two generators, caused by thermal drift. For example, the chip Intel 82802 has two generators (fast and slow), which are located in different parts of the chip and measure the difference in their frequency. Such RNG can be implemented entirely by means of digital logic, because as a rule, inverters with feedback and a chain of buffer elements as a delay line are used as generators. The disadvantages of such generators are:

- the need to place generators at a distance from each other in the chip topology (to reduce the thermal correlation between them);
- low performance (since it is necessary to accumulate the drift for some time of operation);
- not high quality (unpredictability) of random numbers.

In addition, this generator is difficult to implement in FPGA, because automatic development tools do not allow to control the physical placement of generators from each other at a safe distance to reduce the frequency correlation between them.

One of the most crypto-resistant methods of obtaining random numbers in nature are quantum RNGs. In quantum solutions, the entropy of a bit is considered a priori equal to one, taking the position of absolute unpredictability of the value of that bit. Decreasing of quantum bit entropy results from an admixture of classical deterministic chaos. Absolute randomness of a finite sequence may be compromised by a faulty source.

The principle of quantum RNG is based on generating single photons by a light source and directing them to a translucent mirror. The photon may reflect, or it may pass through the translucent mirror with equal probability fates. The choice a photon makes is completely random. At the output of the system are counters that record the number of photons passed and repelled [12].

Most light sources emit photons at random points in time and the number of photons released per unit time is quite random. This fact is the basis of quantum RNGs, built on the basis of a light-sensitive matrix based on CMOS technology of an ordinary camera by a group of scientists from the University of Geneva under the leadership of Bruno Sanguinetti. Each pixel of the matrix counts the number of photons falling on its surface during a certain period of time. These photons are converted into electrons by the corresponding multiplier of the light-sensitive matrix. The number of electrons during the same period will differ by a completely random number [10].

The problem with generators using physical processes is that their analog circuit wastes energy. In addition, it is difficult to keep this analog circuit working because of improvements in the technical process to produce the chips and to miniaturize them. Therefore, it is important to have a fully digital circuit that allows the microprocessor to generate a rich stream of random values without these problems.

The first such RNG solution was proposed in [12], consisting of a circuit with undefined states, which can be in a certain state of logical zero or one. Of course, a digital circuit can detect short periods of time in an undefined state by switching between these two logical values. However, it must work clearly and must never generate between them; otherwise, it would cause delays or even failure in the system [11].

This digitized approach to random discharge generation would work fine if all inverter circuits were absolutely identical. However, the chaos of the physical world never permits this. In fact, no two inverters are exactly alike. The presence of slight differences in the speed or strength of their responses can become a nuisance and jeopardize the randomness of the bit sequence. To keep the inverters in equilibrium, a feedback mechanism is built in. This helps to satisfy one of the rules of statistical randomness: a long stream of numbers must have approximately the same number of all possible digits. By tuning the internal operation of each inverter, you can guard against predictability.

Simultaneously with the development of a robust digital random number source, other Intel engineers developed the additional logic needed to efficiently process and deliver these bit sequences. The unclean bitstream coming from the underlying hardware, regardless of quality, can have bias and correlation.

To guarantee the quality of random numbers, a three-step process is developed that involves an initial digital circuit, a normalizer, and an initial sequence shaper [11]. This three-step random number generation process prevents any predictability variations.

This generator generates a stream of random numbers at a rate of 3 Gb/s. That is, it allows to get rid of the inconvenience of analog components, which are used in physical generators to measure random physical processes, significantly reduce power consumption and increase the rate of generation by more than 30 thousand times. [11].

For the last few years the so-called "autonomous Boolean networks" (ABN) have been actively studied. Such a network is a topologically connected graph of logical elements, to which no control or tact signals are submitted from outside [13; 16].

At the same time, such a network is subject to obvious additional requirements:

- no element can have "hanging" (not connected to any output) inputs;
- no two outputs must be connected to each other.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

These requirements are due to the certainty of the state of the logical elements of the network and the safety of its operation. Depending on the topology, the ABN may exhibit different behavior:

- to be in a stable or quasi-stable state;
- generate with a certain frequency and waveform;
- to be in a state of so-called "Boolean chaos".

An example of the simplest ABN is a repeater with the output connected to the input. Such a network is in a quasi-stable state: depending on the initial state (0 or 1) it will stay in it indefinitely. Another example is one or more inverters connected to each other in a ring. Depending on the number of inverters in the ring, their behavior will be stable, quasi-stable or oscillating.

One inverter is likely to be in a stable state between 0 and 1. This is due to the physical implementation of the inverter as a high gain amplifier with negative feedback equal to 1. For the same reason the lack of generation in very small networks with elements with low output slew rate is possible. With an odd number of inverters, the network will generate with a period proportional to the number of inverters. With an even number of inverters the network is in a quasi-stable state. Obviously, the random number generator implemented in the chip Intel 82802 on two generators and measuring the frequency drift between them, in fact, is a special case of ABN - it uses two rings with a different odd number of inverters. More complex networks can often produce chaotic behavior.

There is a direct physical analogy in content that helps to clearly understand the behavior of the ABN in various situations. It is a pendulum. A simple pendulum, when deflected and released, begins to generate with a stable period - generator behavior. If we flip the pendulum upward, the upper point is a quasi-stable state: at any small deflection, the pendulum will fall to the left or right. If we divide the arm of a pendulum into two parts connected by a hinge, we get a so-called chaotic pendulum whose evolution over time cannot be accurately predicted because any infinitesimal change in the initial state (up to the quantum level) increases with time and leads to quite large changes in the behavior of the pendulum. By this analogy, it is possible to measure random deviations in the frequency of two pendulums arising due to chaotic external influences, but this requires a long analysis, while it is possible to deflect a chaotic pendulum and obtain a random value in the shortest time.

Thus, oscillating ABNs can indeed be used to generate random numbers, but ABNs that initially exhibit chaotic behavior are much more promising. The rate of onset of Boolean chaos and its qualitative characteristics are determined by a number of factors. The most important characteristic is the Lyapunov exponent. If its exponent is negative, the deviations fade with time. If it is greater than zero, the random deviations are exacerbated by the system. If it is zero, the deviations do not fade or intensify, but accumulate if they enter the system from the outside. For rapid physical generation of random numbers, the index must be positive. A simple pendulum has a negative Lyapunov exponent. This is expressed in the fact that the frequency of oscillation is momentarily stabilized due to the absence of external influences.

A chaotic pendulum is a separate example of a system with a positive exponent, so that any small influence leads to a completely different dynamic in a short time. In binary logic, there are no logic functions that amplify small deviations, but there are functions that allow the changes to disappear. For the case with two arguments these are the XOR (exclusive OR) and XNOR (equivalence) functions. Any change in any input signal in them causes a change in the output signal, so these functions are mostly used in RNG.

In binary logic, there are no logical functions that amplify small deviations, but there are functions that do not allow changes to disappear. For the case with two arguments these are the functions XOR (excluding "or") and XNOR (equivalence). Any change in any input signal in them causes a change in the output signal, so these functions are mostly used in RNG.

In modern science, ABN circuits are known to exhibit chaotic behavior. Chaos occurs when the operation of the network is determined by the smallest deviations in the supply voltage, the landslide fronts through thermal fluctuations, surges and other factors that destabilize the network. In the literature [13] two and three input XOR or XNOR logic elements are considered, in which the output is brought back to the inputs via two (or three) delay lines.

In such networks, chaotic behavior can be observed with a certain ratio of delay line lengths. The problem of the network is the strong dependence of the behavior not only on the ratio of delay line lengths, but also on their physical implementation. In this case, instead of chaos, oscillations may occur. In addition, despite the apparent schematic simplicity of the device, it requires a large number of logic elements, because each delay line is a chain of inverters. As a result, a seemingly simple circuit can contain several dozen elements. Moreover, three out of four variants of such an generator have a fundamental disadvantage - the disappearance of the generation after some time. The XOR element comes to a stable state with zero at the output regardless of the number of inputs, and the XNOR element with two inputs comes to a stable state with one at the output. An XOR element with three inputs has an additional stable state with one at the output.

In [16] it is shown that the construction of a true random number generator, containing a digital chaotically oscillating autonomous Boolean network as a source of entropy, should be focused on providing an increase in the rate of number generation while reducing the energy consumption by constructing such partially controlled ABN, which at minimum size is guaranteed and with maximum possible speed enters the Boolean chaos state. The most important requirement should be the impossibility of stable, quasi-stable or oscillating state of the network.

The rate of chaos growth depends directly on the size of the cyclic signal propagation paths available in the network. The larger the path size, the longer it takes for the signal to propagate through it in order to return to the starting point. This means that the network must have a minimum size. This is obvious from the point of view of an generator consisting of an odd number of inverters: the

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

period of oscillation is directly proportional to the length of the ring.

To address these issues, it is better to consider a synchronous network. In fact, the difference between the synchronous Boolean network and ABN is that the signal at the outputs of all logical elements changes simultaneously, so we can assume that the network goes through a series of states.

It was shown in [13] that mutual influence of different network fragments can lead to their forced synchronization. This is a very important effect, which must be excluded or minimized. Since it is necessary to find the minimum possible network, network variants can be analyzed in order of increasing number of logical elements. A network of at least three elements is needed for chaotic behavior. In general, these must be two or three input elements, since the presence of an element with one input turns the network into a network with two elements. To find the necessary network, you can immediately discard all networks with the presence of a stable state. Also immediately excluded are all networks in which the cycle has less than eight states, since in such networks oscillations and cross-effects are possible.

This leaves only the networks evolving through all eight states. A total of 7! = 5040 different cycles is possible, starting at state 000, going through all possible states and through eight iterations back to state 000. These networks simultaneously have a record low level of complexity. For only eight of them, it is possible to modify the nature of the generation so that they satisfy all of the above requirements and have circuit options. They all consist of three logic elements: two XOR elements (block 4) or XNOR elements (block 5) and one initial three-input element with a more complex, special function called "unit count - block 3" (figures 1., 2., 3. accordingly)[16].

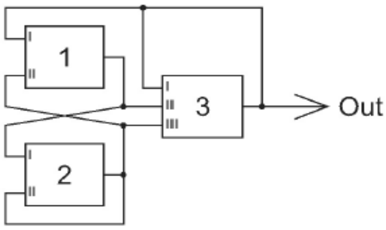


Fig. 1. Functional scheme of the autonomous Boolean network

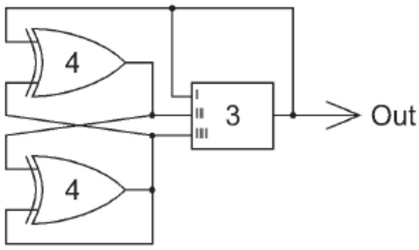


Fig. 2. Logic scheme of an autonomous Boolean network using XOR elements

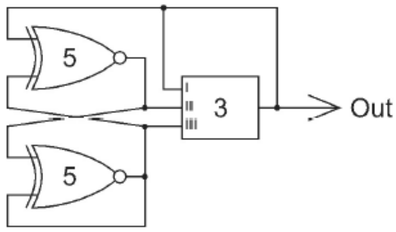


Fig. 3. Logic scheme of an autonomous Boolean network using XNOR elements

Each of the described Boolean networks is a basic unit, on which the random number generator is built. Let's call this basic block "chaotic generator". It has output and modulation input. To reduce the mutual correlation of the signal, the chaotic signal must be removed from the unit count element.

ABN is always in a state of chaotic oscillation and consumes energy in the process. To stop the generation, it is necessary to change the network so that at any initial state it is guaranteed to come to a single possible deterministic state. For the specified networks this cannot be achieved by turning off only one logical element. You need to turn off at least two elements and in the best case these are the same input elements XOR or XNOR. Network can be turned off by forcing the outputs of these elements either to the value 0 or to the value 1. In this case, if the outputs of the XOR/XNOR elements are set to 0, the network output will be set to the value 1, and vice versa.

The chaotic generator itself cannot be used as a random number generator, because it has only an asynchronous output, on which there is a broadband chaotic analog signal. function. On the one hand, it provides a stable initial logic signal, on the other hand, it preserves the previous state, which, if desired, can be used via modulation inputs to produce the next random number.

It should be noted that in spite of mutual modulation, the units of a synchronous chaotic generator can have a shift in the distribution between the number of zeros and ones at the output, i.e. the appearance of one type of quantity at the output is more likely than the other. This is also due to the peculiarities of the physical operation of the logical parts of the circuit. To eliminate this landslide, a procedure called "whitening" of the obtained random numbers may be required.

Thus, ABNs allow you to create RNGs with unique characteristics:

1. The resulting numbers are truly random, which allows them to be used for cryptographic purposes.

2. The rate of random number generation is so high that the network behavior is unpredictable already for the time of signal propagation through several logical elements. That is, when implemented in microprocessor systems, a random number can be obtained in one clock cycle. Such a generation speed actually satisfies any possible needs.

3. the modulation input allows to further improve the characteristics, because another random number can be fed to it. This forces the network to start from a new state each time.

4. The same input allows cross modulation of the discharges of the proposed generator, thereby increasing the rate of chaos buildup.

5. The minimum size of the network makes the proposed generator the most economical in terms of power consumption.

6. The considered generator can be implemented equally effectively on discrete elements, as well as in an integrated design.

7. The generator design is simple and the cost of its implementation is low, which allows it to be used to

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

support cryptography in devices of low resource and energy-saving devices of the Internet of Things.

It should be noted that ABNs require external synchronization to update the device state, and their state spaces are finite and discrete. Meanwhile, ABNs have continuous state spaces, fast time scales, and complex dynamics. ABNs are systems whose future behavior is determined by past times and transient states. Thus, they can be used in various applications such as random number generation [19], genetic schemes [20], etc. In addition, current systems generating Boolean chaos are usually based on discrete logic elements and have a Boolean chaos bandwidth up to 1.4 GHz [15], and in integrated designs up to 3 GHz [11]. Therefore, due to not the fastest electronic signal processing speed, the bandwidth of Boolean chaos remains limited, which has a direct impact on the prospects of ABN applications.

A promising direction of ABN development is the use of optical logic gates to build optical ABNs. Various groups of manufacturers have already proposed a solution to build optical logic gates based on semiconductor optical amplifiers. Such circuits offer the key advantages of high nonlinear coefficients and easy integration. However, so far they have been used only for information processing in optical communication systems, and not for broadband chaos and complex signals.

In [21] we propose an optical ABN device based on optical logic gates, consisting of an optical logic gate XNOR with two feedback links. By adjusting the delay difference between the two channels the system outputs an optical logic chaotic signal. Such logical chaotic signals with high bandwidths solve the problem of Boolean chaos, which can significantly expand the application area of ABM. The paper [21] describes in detail the physical mechanism of optical Boolean chaos and discusses the effects of feedback delay time, carrier optical amplifier recovery time, and power detection. Embedded integration of the optical Boolean chaotic system can be realized through a combination of optical logic gate integration technology and optical delay line integration technology. Simulation results show that this structure can generate not only periodic, controlled rectangular signals, but also chaotic optical Boolean signals with bandwidths up to 14 GHz.

3. Classification of attacks on random number generators

To strengthen security systems and effectively protect cryptosystems, an important scientific and technical task is to analyze various methods of RNG attack and determine countermeasures to eliminate the consequences of such attacks.

An RNG attack aims to reveal generator parameters for further random number prediction. A successful RNG attack can compromise the cryptographic security of the entire IoT network. Therefore, the use of poor quality RNGs simplifies the complexity of attacks. RNGs in cryptographic systems must meet the following requirements: effective hardware and software implementation; true random statistical sequence, cryptographic attack resistance.

Based on the analysis performed in fig. 4. the most common classification of known classes and types of attacks on RNG [22].

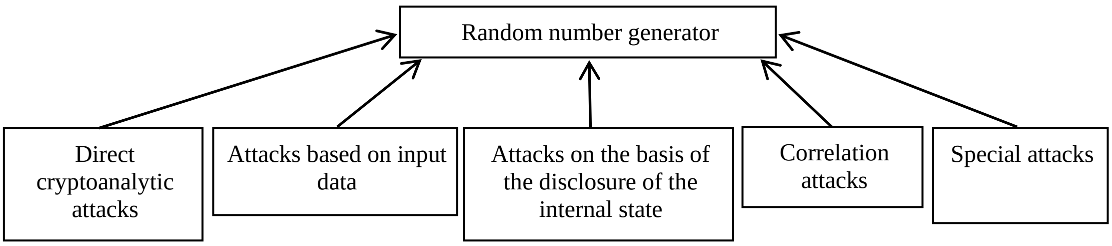


Fig. 4. Classification of attacks on random number generators

The direct cryptanalytic attacks are connected with tracing the initial RNG data and investigating the patterns of its occurrence. These include partial precalculation and temporal attacks. The partial precalculation attack is used based on the analysis of the internal states of the generator and the observation of consistent raw data. The temporal attack is implemented through tracking the pattern of different amount of time in the change of generator states [23].

Input-based attacks are divided into reproducible input attacks, known input attacks and selected input attacks. Known input attacks are implemented by observing input devices or by input entropy number. Attacks with selected inputs are based on the manipulation of generator inputs. Attacks with reproducible input data are based on the same data as the types of this class are considered [24].

Attacks based on internal state disclosure are possible in four variants: permanent compromise attack (based on the disclosure of RNG state at a point in time), return attack (performed in order to restore the RNG states), iterative guessing attack (uses knowledge of RNG state at a point in time and its intermediate) outputs in order to know the state at the next point in time) and "meet in the middle" attack (is essentially a combination of iterative guessing attack and return attack). This class of attack is successful when the initial state of the RNG is known or provided [23].

Correlation attacks are based on the detection of correlation relationships in the original generator sequence. These attacks are the most common attacks [24]. They include the following attacks: fast correlation attack; basic correlation attacks; attacks based on the use of convolutional and turbo codes; attacks based on the recovery of linear polynomials.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

The fast correlation attack based on the parity-check decoding method is the most complex. The basic correlation attack requires high computational complexity. Convolutional and turbo code attacks ask for huge memory overheads. An attack based on linear polynomial reconstruction is considered the most common.

The class of *special attacks* includes: algebraic attacks, analytical attacks, statistical attacks and repetitive attacks. Algebraic attacks analyze vulnerabilities in the internal algebraic structure. Analytical attacks are based on the detection of structural weaknesses in generators. Statistical attacks are based on comparing the number of 0 and 1 values in a sequence. When performing a repetition attack, the attacker intercepts certain data and then sends it out again, blowing it out as legitimate information. The defense against repetition attacks is the use of sequence numbers and time stamps.

Thus, the analysis of attacks on RNG shows that the attacks have different complexity of their implementation, and therefore require different length of time, computing and other capabilities. At the same time, the details of attack protection should be considered depending on their types, schemes of attack implementation and algorithms of RNG functioning. Here are possible variants of protection against attacks by hashing the initial values of the generator and the initial values of entropy source, periodically changing the internal state of RNG.

4. Testing and evaluating the characteristics of random number generators

RNGs play an important role in the generation of cryptographic keys, initial values in IoT network node authentication schemes, etc. The quality of RNG performance determines the cryptographic strength of the data transmitted in the network [6]. Hence the problem of assessing the quality of random bit sequences RNG, the choice and formation of a system of tools for such verification. Today there is a variety of such tools. In recent decades, the most widely used sets of statistical test packages: D. Knuth, Crypt-X, Diehard, U01; NIST[5].

The first set of statistical tests was the one proposed by D. Knuth. It is based on calculating the value of a statistical criterion and comparing it with tabulated statistical results. The conclusion about the quality of a random sequence is probabilistic. The advantage of tests is their small number and the existence of fast execution algorithms, and the disadvantage is the probabilistic nature in interpreting the results.

Crypt-X statistical tests were developed by researchers at the Australian Security Research Center under a commercial license. The tests support key generators, stream ciphers, and block ciphers. They provide tests for frequency characteristics, sequences of equal bits, linear complexity, sequence complexity, binary derivative, and variable point.

Diehard tests were developed by George Magsaglia to measure the quality of a random number set and are considered one of the most rigorous test sets. This set includes 13 tests. The basis of the tests is to compare the characteristics of the random number sequence of the generator according to the provided specification with the expected values. The disadvantage of the tests is the lack of methods for interpreting their results, heuristic and formation of the evaluation result on a two-point "yes" or "no" scale.

Large library of statistical tests set U01 is implemented in C language. It includes classical tests and some original tests.

The specification and library of the NIST test suite were developed by the US Institute of Standards and Technology in the C language and is considered as a standard [4], which includes 15 tests for the analysis of RNG bit sequences. The feature of the tests is the openness of algorithms and unambiguous interpretation of test results. NIST standard includes requirements and methods of a technological nature and is aimed at solving the problem of statistical quality control of pseudorandom sequences.

Thus, certain statistical test packages have a ready-made software implementation. Their use to evaluate random RNG sequences gives an appropriate level of confidence in their quality. Along with this, the following trends can be noted: the existing number of tests does not provide the solution to the RNG estimation problems from all sides; there are no tests that can be recommended to solve most problems; it is impossible to get a clear conclusion about the randomness of a sequence; all test packages have some limitations or drawbacks. Consequently, the problems of assessing the randomness of RNG sequences are far from being complete and require additional research and improvement of existing approaches. The following issues remain problematic: large length of sequences is required for evaluation; it is impossible to change the parameters of existing test implementations; two-point evaluation ("yes"/"no") of the test result; different language of software packages for testing.

It should be noted that any of the suggested tests, or even the whole package of tests, does not replace cryptanalysis. In this case, preliminary testing is mandatory. A generator, which does not satisfy the testing conditions, is unsuitable. Each of the tests included in the package is focused on searching for a certain type of anomalies in the stream of generated symbols.

The use of application test packages faces a number of serious obstacles. The first one is that they are designed to evaluate already ready generators. In practical work, such devices are developed in stages, gradually bringing them to the level of compliance. The second problem is that each of the tests, which are included in the proposed package, is based on a rather complex theoretical justification, requiring from developers a serious mathematical training and knowledge of various incompatible sections of mathematics. Unfortunately, developers, as a rule, do not give such justification in the instructions attached to the tests. Finally, the third problem is that, although the software provides free access, it is difficult to use it. Most tests involve pre-creation of a file into which a tested pseudorandom sequence is written in the form of 32-bit words, and then

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

the test procedure is run. This is not always convenient and not suitable for all tests, as it requires significant hardware and software resources. In addition, the proposed tests are designed for a particular hardware and software platform.

The listed problems force developers if not to develop their own tests, then to create their own software to implement them. It is convenient to work and can be effectively used in the process of searching for the developed design solution of the generator. Of particular interest are studies on short sequences to obtain adequate results, which is typical for RNG of low-power resources of IoT network nodes [5].

To improve the designed circuits of generators, a method for estimating the number of clock cycles to perform certain operations is used. Let us consider the results of such RNG estimation combined with hardware support of basic cryptographic operations (hashing - MD5/SHA-1/HMAC, encryption - AES/DES/TDES) for major microcontroller companies.

Companies manufacturers have begun to introduce hardware RNGs into microcontrollers. The construction of such generators can be divided into four logical levels: 1) the source of entropy of random bits of hardware noise; 2) the level of processing random bits to eliminate statistical defects; 3) block of random number generation with high-speed high capacity; 4) output buffer to read the sequences in accordance with the generator instructions.

For example, STMicroelectronics corporation on the basis of universal core ARM Cortex-M4F (microcontrollers of STM32F4xx family) has integrated RNG module. That is, a microcontroller with hardware support performs basic cryptographic operations (encryption - AES/DES/TDES, geshing - MD5/SHA-1/HMAC), which significantly increases the cryptographic stability of cryptographic transformations. Evaluation of embedded generator shows, that general level of passability of FIPS-140-2 (Federal Information Processing Standard) tests is 85% [3].

This generator (fig. 5.) is implemented on the basis of analog noise source circuit of two independent generators, over the outputs of which is performed the addition operation modulo 2 (XOR). According to this scheme, generation of 32-bit random number is performed by 40 clock cycles of synchronization signal (RNG_CLK). The scheme provides fault control (clocking and entropy) for random value generation with interrupt signal [25]. More detailed test results of cryptographic quality of embedded RNG are given in [26], where positive results on all 15 randomness tests according to FIPS 140-2 requirements in four initial sequence generation modes are given.

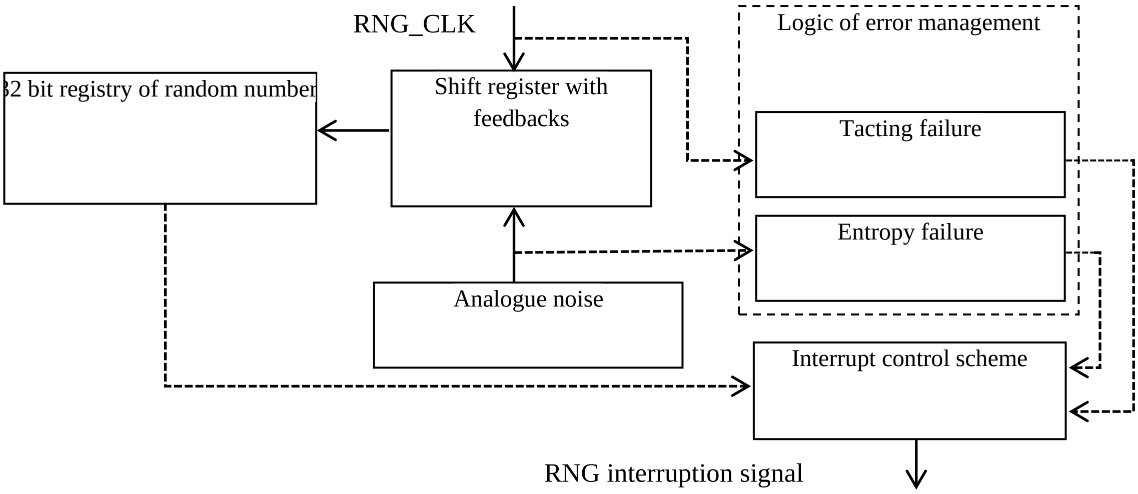


Fig. 5. STM32F2xx/F4xx/F7xx/H7xx RNG microcontroller scheme

In the world of IoT technologies there is a significant security and privacy protection through the development and implementation of general purpose microcontrollers with specialized hardware modules of cryptographic protection of information (cryptoaccelerators). Hardware support for cryptography in IoT devices with cryptoaccelerators allows [26, 28]:

- generate high-quality random number sequences and cryptographic keys;
- store and use cryptographic keys throughout their lifecycle in encrypted form and in secure hardware;
- provide secure personalization (authentication) of IoT devices;
- speed up (tens, hundreds or even thousands of times) the execution of certain crypto-algorithms;
- relieve the CPU from the cryptographic transformation of information;
- provide greater crypto resistance, energy efficiency, and miniaturization of IoT devices.

The core of crypto acceleration engines may include: 1) gas pedals of symmetric encryption based on TDES/AES algorithms, gas pedals of asymmetric cryptography based on RSA and DSA algorithms; 2) gas pedals of hashing based on MD5, SHA-1, SHA-224, SHA-256, HASH algorithms; 3) random number generators based on a physical noise source.

Table 1 shows data from the technical documentation on the number of clock cycles to process one encryption block for the corresponding algorithms: TDES in ECB, CBC modes and AES-128/192/256 in ECB, CBC, CTR, GCM, XTS, GCTR modes. Also in the table to compare performance of cryptoaccelerators for different block sizes with listing by number of clock cycles per byte (cycles per byte - CPB). Besides in the

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

table there is an estimation of performance of cryptoaccelerators in the form of NB parameter as a number of processing bytes for 1 ms at the maximum clock frequency NB = FCPU/(1000×NB).

Comparison of performance of cryptoaccelerators with reproduced means of cryptographic transformations [26] shows their significant advantages. For example, for block AES encryption algorithm performance increases by 10-20 times for 8/16-bit cryptoaccelerators and by 150 times for 32-bit cryptoaccelerators correspondingly. With respect to hash calculation, the performance gain for the SHA-1, SHA-256 algorithms is over 100 times for 32-bit cryptoaccelerators and up to 500 times for NMAS.

In general, there is a trend of hardware support for cryptography in IoT devices with the introduction of comprehensive security solutions, such as identification and authentication of network nodes [27; 28], symmetric and asymmetric encryption, cryptographic protocols, secure key storage and generation, secure application firmware loading and updating, support for digital signatures and certificates, high crypto-resistance and energy efficiency.

Table 1. *Crypto-accelerators speed estimation*

Operation	**CPU**	**Family/model MC**	**FCPU, MHz**	**Modes**	**Tact/ block**	**CPB, tacts/bytes**	**NB, byte**
Evaluation of crypto-accelerator speed performance of 8-bit microcontrollers							
Enc./Dec. AES-128	AVR	XMega	32	ECB, CBC	375	23,4	1 365
Enc./Dec. AES-128	STM8	STM8L16 STM8AL	16	ECB	892	55,8	287
Enc./Dec. AES-128	i8051	C8051F96x	25	ECB, CBC, CTR	218	13,6	1 835
Enc./Dec. AES-256					298	18,6	1 342
Speed estimation of crypto-accelerators for 16-bit microcontrollers							
Enc./Dec. AES-128	MSP430	MSP430F6xx	25	ECB, CBC, OFB, CFB	167	10,4	2 395
Enc./Dec. AES-128		MSP430FR5x	16		168	10,5	1 524
Enc./Dec. AES-256		MSP430FR6x			234	14,6	1 094
Enc./Dec. TDES	PIC24	PIC24FJ64	32	ECB, CBC, OFB, CFB, CTR	26	3,3	9 846
Enc./Dec. AES-128		PIC24FJ128			219	13,7	2 338
Enc./Dec. AES-256		PIC24FJ256			299	18,7	1 712
Evaluation of crypto-accelerator speeds of 32-bit microcontrollers							
Enc./Dec. TDES	ARM7TDMI	SAM 7XC	55	ECB, CBC, OFB, CFB	50	6,3	8 800
Enc./Dec. AES-128				ECB, CBC, OFB, CFB, CTR	12	0,8	73 333
Enc./Dec. AES-256					14	0,9	62 857
Enc./Dec. AES-128	ARM Cortex-M4F	SAM E5x SAM D5x	120	ECB, CBC, OFB, CFB, CTR, GCM	57	3,6	33 684
Enc./Dec. AES-256					77	4,8	24 935
Hash SHA-1					85	1,3	90 353
Hash SHA-256					72	1,1	106 667
TRNG-32					84	21,0	5 714
Enc./Dec. AES-128	ARM Cortex-M7	SAM E70 SAM S70 SAM V70 SAM V71	300	ECB, CBC, OFB, CFB, CTR, GCM	10	0,6	480 000
Enc./Dec. AES-256					14	0,9	342 857
Hash SHA-1					85	1,3	225 882
Hash SHA-256					72	1,1	266 667
TRNG-32					84	21,0	14 286
Enc./Dec. TDES	ARM Cortex-M7F	STM32H7xx	400	ECB, CBC	64	8,0	50 000
Enc./Dec. AES-128				ECB, CBC,CTR,GCM, CCM, GMAC	14	0,9	457 143
Enc./Dec. AES-256					18	1,1	355 555
Hash SHA-1					82	1,3	312 195
Hash SHA-256					66	1,0	387 879
TRNG-32					54	13,5	29 630

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

Conclusions

Protection of IoT solutions includes security of IoT network nodes and their connection to the cloud using secure protocols, confidentiality, authenticity and integrity of data during transmission, processing and storage in the IoT network, as well as resistance to physical and virtual attacks. Information is protected by cryptographic methods (encryption and hashing) using cryptographic keys. The initial basis for the crypto resistance of IoT solutions is the true randomness of the sequences formed by the RNG and used in cryptographic transformation algorithms of information for its protection. The peculiarities of IoT devices are their heterogeneity and territorial distribution, limited computing resources and power supply, miniaturization. Due to the above features of IoT, generation of random sequences by software in a deterministic algorithm in high-performance microprocessor systems is unacceptable. Such sequences are of pseudorandom nature, which means that the possibility of their predictability increases, and, as a result, the crypto resistance of the systems decreases.

The problem of generators that use physical processes is that their analog circuit wastes energy. In addition, it is difficult to maintain the performance of this analog circuit due to improvements in the technical process for the production of chips and their miniaturization. Generators on digital circuits can significantly reduce power consumption and increase the rate of generation by more than 30 thousand times. To guarantee the quality of random numbers, they implement a three-step process, which involves an initial digital circuit, a normalizer and a shaper of the initial flow of random numbers.

Autonomous Boolean networks allow to create RNG with unique characteristics: 1) obtained numbers are really random, which allows to use them for cryptographic purposes; 2) speed of random number generation is so high, that when implemented in microprocessor systems random number can be obtained in one clock cycle; 3) modulation input allows to further improve characteristics, that is allows cross modulation of generator bits, thus increasing speed of chaos increase; 4) minimal network size makes the proposed generator the most economical in terms of power consumption; 5) the generator can be implemented equally effectively on discrete elements, as well as in integrated design; 6) the generator design is simple and the cost of its implementation is low, which allows to use it to support cryptography in low-resource and energy-saving IoT devices with a huge bandwidth of Boolean chaos to 3 GHz.

A promising direction of ABM development is the use of optical logic elements to build optical ABMs, the structure of which consists of an optical logic valve XNOR with two feedback links on the optical delay lines. Simulation results show that this structure can generate not only periodic, controlled rectangular signals, but also chaotic optical Boolean signals with a bandwidth up to 14 GHz.

RNG in cryptographic systems must meet the following requirements: effective hardware and software implementation; true random statistical sequence, cryptographic attack resistance. Classification of attacks on RNG includes the following classes: direct cryptanalytic attacks; attacks based on input data; attacks based on internal state disclosure; correlation attacks and special attacks. Protection against attacks is achieved by hashing the initial values of the generator and the initial values of the entropy source, by periodically changing the internal state of the RNG.

The practical use of statistical test packages to evaluate RNG sequences encounters a number of serious obstacles: they are designed to evaluate ready-made generators, although in practice such devices are developed in stages, gradually bringing them to the level of compliance; each of the tests is based on a fairly complex theoretical foundation, requiring from generator developers a serious mathematical training; most tests involve the prior creation of a file in which a tested pseudorandom sequence is written in the form of 32-bit words, and then the test procedure is run, which is not always convenient, because it requires significant hardware and software resources; the proposed tests are designed for a recognized hardware and software platform.

Comparison of performance of cryptoaccelerators with lost cryptographic transformations shows their significant advantages. For example, for the AES block encryption algorithm, performance increases by a factor of 10-20 for 8/16-bit cryptoaccelerators and by a factor of 150 for 32-bit cryptoaccelerators. With respect to hash calculation, the performance gain for the SHA-1, SHA-256 algorithms for 32-bit crypto gas pedals is 100 times greater, and for NMAS up to 500 times greater.

Proposals for further research are focused on identifying technologies and effective solutions for hardware support of cryptography in IoT devices with implementation of comprehensive security solutions, such as identification and authentication of network nodes, symmetric and asymmetric encryption, cryptographic protocols, secure key storage and generation, secure application loading, support of digital signatures and certificates, high crypto-resistance and energy efficiency.

References

1. Donald Knuth (2011), *The Art of Computer Programming*, Volumes 1-4A Boxed Set, Third Edition, Reading, Massachusetts: Addison-Wesley, 3168p.
2. Bruce Schneier (2015), *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 20th Anniversary Edition. March 784 p.
3. FIPS PUB 140-2 (2001), "Security Requirements for Cryptographic Modules", *Federal Information Processing Standards Publication* 140-2, P. 69.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

4. Elaine Barker, John Kelsey, (2012), "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", *NIST Special Publication* ,No. 800-90A.
5. Popereshnyak, S.V., Raichev, O.O. (2021), "Research and testing of lightweight pseudo-random number generators for the Internet of Things", *Ukrainian scientific journal of information security*, Vol. 27 (2), P. 71–78.
6. Akram, R. N, Markantonakis, K., Mayes, K. (2012), "Pseudorandom Number Generation in Smart Cards: An Implementation, Performance and Randomness Analysis", *5th International Conference on New Tech- nologies, Mobility and Security (NTMS)*, **DOI:** https://doi.org/10.1109/NTMS.2012.6208760.
7. Koning Gans G., Hoepman J.-H., Garcia F. D. A. (2008), "Practical Attack on the MIFARE Classic. CARDIS'08: Proceedings of the 8th IFIP WG 8.8/11.2", *International conference on Smart Card Research and Advanced Applications. Springer*, P. 267–282.
8. Building a Low-Cost White-Noise Generator, "Maxim Integrated. Application note 3469", available at: https://pdfserv.maximintegrated.com/en/an/AN3469.pdf
9. Sovin, Y. R., Nakonechny, Yu. M., Opirsky, I. R., Stakhiv, M. Yu. (2018), "Analysis of cryptography hardware support in IoT devices", *Ukrainian Scientific Journal of Information Security*, Vol. 24, Issue 1, P. 36–48.
10. Anthony Martin, Hugo Zbinden, Nicolas Gisin., "Quantum random number generation on a mobile phone", available at: http://arxiv.org/pdf/1405.0435v1.pdf
11. Greg Taylor, George Cox. (2011), "Behind Intel's new random number generator", IEEE Spectrum. Computing, Hardware. September, available at: http://courses.csail.mit.edu/6.857/2012/files/ieee-spectrum.pdf
12. Mario Stipčević, Çetin Kaya Koç, "True Random Number Generators. ResearchGate. Open Problems in Mathematics and Computational Science", P.275–315. **DOI:** https://doi.org/10.1109/NTMS.2012.620876010.1007/978-3-319-10683-0_12.
13. David P. Rosin, Damien Rontani, Daniel J. Gauthier, and Eckehard Schöll (2013), *Experiments on autonomous Boolean networks*, Chaos 23, 025102.
14. David Rosin., *Dynamics of Complex Autonomous Boolean Networks*, Doctoral dissertation Universität, Technische Berlin, available at: https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/7/38882/files/2016/09/rosin_david-14v7bca.pdf
15. R. Zhang, H. L. D. De, S. Cavalcante, Z. Gao, D. J. Gauthier, J. E. S. Socolar, M. M. Adams, and D. P. Lathrop (2009), "Boolean chaos" Phys. Rev. E 80 (4), 045202.
16. Goncharov, S.V. (2021), *Generator of truly random numbers*, Description of the invention to patent RU2741865C1, P. 24. available at: https://patents.google.com/patent/RU2741865C1/ru
17. Gorbenko, Y. I, Shapochka, N.V, Grinenko, T. O, Neyvanov, A. V, Mordvinov, R. I. (2011), "Methods and means of generating pseudo-random sequences", *Applied radio electronics: scientific and technical. Magazine*, Vol. 10. No. 2. P. 141–152.
18. DSTU ISO / IEC 11770-1: 2014, *Information Technology. Methods of protection*, Security key management, Part 1: Structure [to replace DSTU ISO / IEC 11770-1: 2009].
19. D. P. Rosin, D. Rontani, and D. J. Gauthier (2013), "Ultrafast physical generation of random numbers using hybrid Boolean networks", Phys. Rev. E 87 (4), 040902.
20. X. Cheng, M. Sun, and J. E. S. Socolar (2013), "Autonomous Boolean modelling of developmental gene regulatory networks " J. R. Soc., Interface 10 (78), 20120574.
21. Luxiao Sang, Jianguo Zhang, Tong Zhao, Martin Virte, Lishuang Gong, and Yuncai Wang (2020), "Optical Boolean chaos", *Optics Express 29296*, Vol. 28, No. 20/28. available at: https://opg.optica.org/oe/fulltext.cfm?uri=oe-28-20-29296&id=439748
22. Mandrona, M., Garasimchuk, O. (2012), "Attacks on pseudo-random number generators", *Visn. Nat. Lviv Polytechnic University*, No. 741, P. 251–256.
23. Rock, A. (2005), *Pseudorandom Number Generators for Criptographic Applications*, Salzbuburg, 57–65p.
24. Zenner, E.(2004), *On Cryptographic Properties of LFSR-based Pseudorandom Generators*, Mannheim, 102p.
25. "Reference manual" (2011), STM32F405xx, STM32F407xx, STM32F415xx and STM32F417xx advanced ARM-based 32-bit MCUs (RM0090), STMicroelectronics, 1316 p.
26. Sovin, Y. R., Nakonechny, Yu. M., Chinka, V. M., Tyshik, I. Y. (2012), "Testing of the built-in random number generator of microcontrollers of the STM32F4XX family according to the NIST STS method", *Lviv Polytechnic National University, Department of Information Protection*, P. 168–175.
27. Klimushin, P., Solianyk, T., Kolisnyk, T., Mozhaev, O. (2021), "Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things", *Advanced Information Systems*, Vol. 5, No. 3, P. 103–111.
28. Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov V. (2021), "Hardware support procedures for asymmetric authentication of the internet of things", *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (18), P. 31–39.

Received 24.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Клімушин Петро Сергійович – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: klimushyn@ukr.net; ORCID: https://orcid.org/0000-0002-1020-9399.

Климушин Петр Сергеевич – кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Petro Klimushyn – Candidate of technical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Соляник Тетяна Миколаївна – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: t.solianyk@khai.edu; ORCID: https://orcid.org/0000-0003-3695-0019.

Соляник Татьяна Николаевна – кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Tetiana Solianyk – Candidate of technical science, associate professor, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Можаєв Олександр Олександрович – доктор технічних наук, професор, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: mozhaev1957@gmail.com; ORCID: https://orcid.org/0000-0002-1412-2696.

Можаев Александр Александрович – доктор технических наук, профессор, профессор кафедры кибербезопасности и DATA-технологий, Харьков, Украина.

Oleksandr Mozhaiev – Doctor of technical science, professor, professor of Cyber Security and DATA-Technologies Department, Kharkiv, Ukraine.

Гнусов Юрій Валерійович – кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та DATA-технологій, Харків, Україна; e-mail: duke6969@i.ua; ORCID: http://orcid.org/0000-0002-9017-9635.

Гнусов Юрий Валерьевич – кандидат технических наук, доцент, заведующий кафедрой информационных технологий и DATA-технологий, Харьков, Украина.

Yurii Gnusov – Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Technologies and DATA-Technologies, Kharkiv, Ukraine.

Манжай Олександр Володимирович – кандидат юридичних наук, доцент, завідувач кафедри протидії кіберзлочинності, Харків, Україна; e-mail: sofist@ukr.net; ORCID: https://orcid.org/0000-0001-5435-5921.

Манжай Александр Владимирович – кандидат юридических наук, доцент, заведующий кафедрой противодействия киберпреступности, Харьков, Украина.

Oleksandr Manzhai – Candidate of Legal Sciences,, Associate Professor, Head of the Department for Combating Cybercrime, Kharkiv, Ukraine.

Світличний Віталій Анатолійович – кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: vit.svet@ukr.net; ORCID: https://orcid.org/0000-0003-3381-3350

Светличный Виталий Анатольевич – кандидат технических наук, доцент, доцент кафедры противодействия киберпреступности, Харьков, Украина.

Vitaliy Svitlychny – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Combating Cybercrime, Kharkiv, Ukraine.

КРИПТОСТІЙКІ МЕТОДИ ТА ГЕНЕРАТОРИ ВИПАДКОВИХ ЧИСЕЛ У ПРИСТРОЯХ ІНТЕРНЕТ РЕЧЕЙ (IOT)

Предмет дослідження: криптостійкі методи та засоби генерування випадкових послідовностей та апаратна підтримка криптографічних перетворень у пристроях IoT. **Метою** статті є дослідження криптостійких методів та засобів генерування та тестування випадкових послідовностей, придатних для використання у пристроях IoT з обмеженими ресурсами; визначення схемних реалізацій апаратних генераторів випадкових послідовностей; формування висновків щодо використання генераторів випадкових чисел (ГВЧ) в системах криптографічного захисту мережі IoT. У статті вирішуються наступні **завдання:** аналіз методів та апаратних засобів формування випадкових послідовностей для захисту рішень IoT з обмеженими ресурсами; визначення безпечних та ефективних технологій реалізації ГВЧ; класифікація атак на ГВЧ; аналіз перешкод практичного використання пакетів статистичних тестів для оцінювання якості випадкових послідовностей ГВЧ; оцінювання швидкодії криптоакселераторів апаратної підтримки криптографічних перетворень; надання практичних рекомендацій щодо RNG для застосування в пристроях IoT з обмеженими ресурсами. **Методи** дослідження: метод структурно-функціонального аналізу RNG та пристроїв IoT, криптографічні методи захисту інформації, методи генерування випадкових послідовностей, метод аналізу стійкості систем, методи побудови автономних булевих мереж та аналізу булевого хаосу, методи оцінювання якості випадкових послідовностей. **Результатами** роботи є аналіз технологій та схемних рішень апаратних ГВЧ за характеристиками: якість випадковості чисел та непередбаченість послідовностей, швидкодія, енергоспоживання, мініатюрність, можливість інтегрального виконання; надання практичних рекомендацій щодо для застосування ГВЧ в системах криптографічного захисту мережі IoT. **Новизною** проведеного дослідження є аналіз методів та апаратних засобів підтримки технологій генерування випадкових послідовностей в системі криптографічного захисту рішень IoT; проведення класифікації атак на ГВЧ та особливостей захисту від них; визначення ефективних технологій та схемних рішень ГВЧ щодо використання в малопотужних пристроях IoT з обмеженими обчислювальними ресурсами; надання практичних рекомендацій щодо використання ГВЧ в системах криптографічного захисту мережі IoT. Аналіз технологій та схемних рішень дозволив сформувати наступні **висновки:** захист рішень IoT включає: безпеку вузлів мережі IoT та їх підключення до хмари за допомогою захищених протоколів, забезпечення конфіденційності, автентичності та цілісності даних в мережі IoT криптографічними методами, аналіз атак та моніторинг криптостійкості мережі IoT; первісною основою захисту рішень IoT є істинна випадковість послідовностей, які формуються ГВЧ і використовуються у алгоритмах криптографічного перетворення інформації для її захисту; особливістю пристроїв IoT є їх гетерогенність і географічний розподіл, обмеженість обчислювальних ресурсів та електроживлення, мініатюрність; найбільш ефективними (зменшують енергоспоживання та збільшують швидкість генерації) для застосування в пристроях IoT є RNG виключно на цифровій основі, в яких реалізується триступінчастий процес: початкова цифрова схема, нормалізатор та формувач потоку випадкових чисел; автономні булеві мережі (АБМ) дозволяють створити RNG з унікальними характеристиками: отримані числа є дійсно випадковими, висока швидкість – число можна отримати за один такт, мінімальне енергоспоживання, мініатюрність, висока (до 3 ГГц) пропускна здатність булевого хаосу; перспективним напрямом розвитку АБМ є використання оптичних логічних вентилів для побудови оптичних АБМ з пропускною здатністю до 14 ГГц; класифікація відомих класів атак на ГВЧ включає: прямі криптоаналітичні атаки, атаки, засновані на вхідних даних, атаки на основі розкриття внутрішнього стану ГВЧ, кореляційні атаки та спеціальні атаки; пакети статистичних тестів для оцінювання

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

послідовностей RNG мають деякі обмеження або недоліки та не замінюють криптоаналіз; порівняння швидкодії криптоакселераторів з програмними засобами криптографічних перетворень показує їх значні переваги: для блокового алгоритму шифрування AES підвищується швидкодія в 10-20 разів у 8/16-бітових криптоакселераторах і в 150 разів у 32-бітових, хешування зростання швидкодії для алгоритмів SHA-1, SHA-256 у 32-бітових криптоакселераторів більш ніж в 100 разів, а для алгоритму HMAC – до 500 разів.

Ключові слова: інтернет речей; генератор випадкових чисел; криптостійкість; криптоаналіз; криптографічні ключі; шифрування; хешування; автономні бульові мережі; булевий хаос; статистичні тести; криптоакселератори.

КРИПТОСТОЙКИЕ МЕТОДЫ И ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ В УСТРОЙСТВАХ ИНТЕРНЕТ ВЕЩЕЙ (IOT)

Предмет исследования: криптостойкие методы и способы генерирования случайных последовательностей и аппаратная поддержка криптографических преобразований в устройствах IoT. **Целью** статьи является исследование криптостойких методов и средств генерирования и тестирования случайных последовательностей, пригодных для использования в IoT устройствах с ограниченными ресурсами; определение схемных реализаций аппаратных генераторов случайных последовательностей; формирование выводов по использованию генераторов случайных чисел (ГСЧ) в системах криптографической защиты сети IoT. В статье решаются следующие **задачи:** анализ методов и аппаратных средств формирования случайных последовательностей для защиты решений IoT с ограниченными ресурсами; определение безопасных и эффективных технологий реализации ГСЧ; классификация атак на ГСЧ; анализ недостатков практического использования пакетов статистических тестов для оценивания качества случайных последовательностей ГСЧ; оценивание быстродействия криптоакселераторов аппаратной поддержки криптографических преобразований; предоставление практических рекомендаций по ГСЧ для применения в устройствах IoT с ограниченными ресурсами. **Методы** исследования: метод структурно-функционального анализа ГСЧ и устройств IoT, криптографические методы защиты информации, методы генерирования случайных последовательностей, метод анализа устойчивости систем, методы построения автономных булевых сетей и анализа булевого хаоса, методы оценивания качества случайных последовательностей. **Результаты** работы: анализ технологий и схемных решений аппаратных ГСЧ по следующим характеристиками: качество случайности чисел и непредсказуемость последовательностей, быстродействие, энергопотребление, миниатюрность, возможность интегрального выполнения; предоставление практических рекомендаций по применению ГСЧ в системах криптографической защиты сети IoT. **Новизной** проведенного исследования является анализ методов и аппаратных средств поддержки технологий генерирования случайных последовательностей в системе криптографической защиты решений IoT; проведение классификации атак на ГСЧ и особенностей защиты от них; определение эффективных технологий и схемных решений ГСЧ по использованию в маломощных устройствах IoT с ограниченными вычислительными ресурсами; предоставление практических рекомендаций по использованию ГСЧ в системах криптографической защиты сети IoT. Анализ технологий и схемных решений позволил сформировать следующие **выводы:** защита решений IoT включает: безопасность узлов сети IoT и их подключение к облаку с помощью защищенных протоколов, обеспечение конфиденциальности, подлинности и целостности данных в сети IoT криптографическими методами, анализ атак и мониторинг криптостойкости сети; первоначальной основой защиты решений IoT является истинная случайность формируемых ГСЧ последовательностей и используемых в алгоритмах криптографического преобразования информации для ее защиты; особенностью устройств IoT является их гетерогенность и географическое распределение, ограниченность вычислительных ресурсов и электропитания, миниатюрность; наиболее эффективными (уменьшают энергопотребление и увеличивают скорость генерации) для применения в устройствах IoT являются ГСЧ исключительно на цифровой основе, в которых реализуется трехступенчатый процесс: начальная цифровая схема, нормализатор и формирователь потока случайных чисел; автономные булевые сети (АБС) позволяют создать ГСЧ с уникальными характеристиками: полученные числа действительно случайные, высокая скорость – число можно получить за один такт, минимальное энергопотребление, миниатюрность, высокая (до 3 ГГц) пропускная способность булевого хаоса; перспективным направлением развития АБМ есть использование оптических логических вентилей для построения оптических АБС с пропускной способностью до 14 ГГц; классификация известных классов атак на ГСЧ включает: прямые криптоаналитические атаки; атаки, основанные на входных данных; атаки на основе раскрытия внутреннего состояния ГСЧ; корреляционные атаки и специальные атаки; пакеты статистических тестов для оценивания последовательностей ГСЧ имеют некоторые ограничения или недостатки и не заменяют криптоанализ; сравнение быстродействия криптоакселераторов с программными средствами криптографических преобразований показывает их значительные преимущества: для блочного алгоритма шифрования AES повышается быстродействие в 10-20 раз в 8/16-битовых криптоакселераторах и в 150 раз – в 32-битовых, хеширования роста SHA-256 у 32-битных криптоакселераторов более чем в 100 раз, а для алгоритма HMAC – до 500 раз.

Ключевые слова: интернет вещей; генератор случайных чисел; криптостойкость; криптоанализ; криптографические ключи; шифрование; хеширование; автономные булевые сети; булевый хаос; статистические тесты; криптоакселераторы.

Бібліографічні описи / Bibliographic descriptions

Клімушин П. С., Соляник Т. М., Можаєв О. О., Гнусов Ю. В., Манжай О. В., Світличний В. А. Криптостійкі методи та генератори випадкових чисел у пристроях інтернет речей (IOT). *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 22–34. DOI: https://doi.org/10.30837/ITSSI.2022.20.022

Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., Svitlychny, V. (2022), "Crypto-resistant methods and random number generators in internet of things (IOT) devices", *Innovative Technologies and Scientific Solutions for Industries,* No. 2 (20), P. 22–34. DOI: https://doi.org/10.30837/ITSSI.2022.20.022

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

UDC 004.056.55:004.312.2 DOI: https://doi.org/10.30837/ITSSI.2022.20.035

N. LADA, Y. RUDNYTSKA

IMPLEMENTATION OF A METHOD FOR SYNTHESIZING GROUPS OF SYMMETRIC DOUBLE-OPERAND OPERATIONS OF CRYPTOGRAPHIC INFORMATION CODING FOR BLOCK ENCRYPTION SYSTEMS

The **object** of the study is the processes of building groups of symmetric double-operand operations of cryptographic coding of information. The **subject** of the study are features of the implementation of a generalized method of synthesis groups of symmetric two-operand operations of cryptographic coding information for "lightweight cryptography". The purpose of this work is to investigate the process of building and implementing a method of synthesis of groups of symmetric multibit double-operand operations of information cryptographic coding to provide automation for finding ways to increase the variability, and stability of lightweight cryptoalgorithms. The following **tasks** are solved in the article: to determine the mathematical group of single-operand operations, on the basis of which the realization of the method of synthesis of groups of symmetric double-operand operations of cryptographic coding will be presented; to offer the search technology of symmetric double-operand operations; to evaluate power of synthesized groups of operations, and their influence on variability and stability of " lightweight cryptography" algorithms. The following **results** were obtained: the technology for determining symmetric double-operand operations, which will be the basis for the synthesis of a group of symmetric double-operand operations, was proposed. A method for synthesizing groups of symmetric double-operand cryptographic information coding operations for block encryption systems was proposed and implemented. On the example of module-two addition with correction and the use of three-digit single-operand operations, the practical implementation of this method was shown. Based on the synthesized operations and the given quantitative characteristics of the set of single-operand operations, the power of synthesized groups of operations and their influence on the variability and stability of "lightweight cryptography" algorithms were evaluated. **Conclusions:** the proposed and implemented method of synthesis of groups of symmetric double-operand operations of cryptographic coding information allows to provide the possibility of increasing the variability of lightweight crypto-algorithms. Synthesis of symmetric cryptographic coding operations belonging to different mathematical groups provides increase of algorithm's crypto stability. Application of synthesized cryptographic coding operations leads to significant increase of variability of cryptoalgorithms and their complexity.

Keywords: cryptographic encoding; lightweight cryptography; synthesis of symmetric operation groups.

Introduction

Statement of the problem. The development of information technology and the digitalization of society have led to the need to process large amounts of data in real time. However, there are a number of applications of information technology related to the need to process sensitive information with limited resources. To solve these problems traditional crypto-algorithms were not effective enough [1 - 3]. Their solution is the use of "lightweight cryptography" using cryptographic coding operations. This approach provides both theoretical and practical solution to the important scientific and technical problem of providing protection of personal information resources and secure functioning of personal information management systems under existing hardware limitations.

Analysis of recent research and publications

The development of lightweight cryptoalgorithms is conducted mainly in the direction of using special restrictions of traditional algorithms on the block size, number of internal states, simplification of rounds algorithms and their number [3, 5 - 7]. However, it should be noted that the development of lightweight cryptoalgorithms focuses on block-based crypto algorithms [8].

The second way of developing "lightweight cryptography" is to build crypto-algorithms based on cryptographic coding operations [9, 10]. Synthesized cryptographic coding operations based on discrete substitution table models implement both linear and nonlinear information transformations [11, 12].

Among cryptographic coding operations, a special place belongs to double-operand operations, which provide a random implementation of substitution tables. [13, 14]. Among a variety of double-operand operations it is reasonable to allocate symmetric double-operand operations [15, 16], which can find wide application both in block and stream encryptions.

However, at present multi-digit double-operand operations of cryptographic conversion remain insufficiently investigated. It should be noted that the digit capacity of double-operand operations means the minimum amount of information to be converted [13]; the units of the minimum amount of information can be bits, bytes, words, etc.

The **aim** of the article. To study the process of construction and implementation of the method of synthesis of groups of symmetric multi-digit double-operand operations of cryptographic coding of information to provide automation of finding ways to increase the variability of lightweight cryptoalgorithms.

Main part

A double-operand cryptographic encoding operation is an operation, which converts the value of the first operand based on one of several single-operand operations, depending on the value of the second operand. In other words, a double-operand operation is a formalized tuple of single-operand operations from which only the single-operand operation whose ordinal number is determined by the second operand will be implemented

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

for information conversion.

If at identical values of the second operand the two-operand operation realizes both direct and reverse cryptographic transformation, this operation will be symmetric.

Let us consider synthesis of symmetric three-digit two-operand cryptographic coding operations.

The number of single-operand cryptographic encoding operations is defined [10].

$$K_o^1(n) = 2^n!, \quad (1)$$

$$K_o^1(n) = K_{\text{об}}(n) \cdot K_{\text{оп}}(n) \cdot K_{\text{ои}}(n) = K_{\text{об}}(n) \cdot n! \cdot 2^n \quad (2),$$

where n – operation digit, $K_{\text{об}}(n)$, $K_{\text{об}}(n) \cdot n!$, $K_{\text{ои}}(n) = 2^n$ the number of basic operations, transposition operations, and inversion operations, respectively.

Based on expressions (1) and (2) the number of two-digit single-operand cryptographic coding operations is defined [9]:

$$K_o^1(2) = 4! = 24.$$

$$K_o^1(2) = K_{\text{об}}(2) \cdot 2! \cdot 2^2 = 3 \cdot 6 \cdot 4 = 24.$$

Since, according to the results of the experiment, there are 96 symmetric two-digit double-operand operations, and they make up 4 groups of 24 operations, we can assume that: $K_o^2(2) = 96 = 4 \cdot 2^2!$. So,

$$K_o^2(n) = k \cdot 2^n! \quad (3)$$

where k – number of groups of symmetric n-digit double-operand cryptographic coding operations.

The number of operations in each group of symmetric three-digit two-order operations according to (3) is defined: $K_o^2(3) = k \cdot 2^3! = k \cdot 8!$ and is 40 320 operations [17].

In practice, it is currently impossible to synthesize a group of such a number of operations. This is due to the lack of a single mathematical apparatus allowing to simulate the whole set of three-digit single-operand operations [10]. Therefore, in the process of synthesis of symmetric three-digit two-operand operations we will limit ourselves only to synthesis of basic double-operand operations based on matrix single-operand operations.

According to [17], the number of basic three-digit single-operand matrix operations is 28 operations. These operations are presented in table 1.

Table 1. *Basic group of three-digit single-operand matrix cryptographic coding operations*

$F_1^k = F_1^d = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$	$F_8^k = F_8^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$	$F_{15}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{22}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$
		$F_{15}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{22}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$F_2^k = F_2^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix}$	$F_9^k = F_9^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{16}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
		$F_{16}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
$F_3^k = F_3^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$	$F_{10}^k = F_{10}^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{17}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{24}^k = F_{24}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$
		$F_{17}^d = \begin{pmatrix} x_1; \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	
$F_4^k = F_4^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$	$F_{11}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{18}^k = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{25}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$
	$F_{11}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{18}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{25}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

The end **Table 1**

$F_5^k = F_5^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{12}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{19}^k = F_{19}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{26}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{12}^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}$		$F_{26}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix}$
$F_6^k = F_6^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$	$F_{13}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_2 \end{pmatrix}$	$F_{20}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{27}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{13}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$	$F_{20}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$	$F_{27}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
$F_7^k = F_7^d = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{14}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{21}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{28}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$
	$F_{14}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{21}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$	$F_{28}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$

Therefore, in the process of synthesis of symmetric three-digit double-operand matrix operations of cryptographic coding we will use numbering of single-operand operations according to table 1.

To develop and implement the method of synthesis of groups of symmetric double-operand operations of cryptographic coding information for block encryption systems it is necessary to establish a symmetric double-operand operation based on which we will conduct the synthesis.

Let us consider in more detail the operation $O_1^{4\oplus}$, on the basis of which the synthesis of the fourth group of symmetric two-operand operations of cryptographic coding was performed [15]:

$$O_1^{4\oplus} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix} \qquad (4)$$

Based on expression (4), the operation $O_1^{4\oplus}$ can be called a bitwise addition operation module-two with correction.

When developing the method of synthesis of groups of symmetric double-operand operations of cryptographic coding synthesis was performed on the basis of operations:

1) module-two additon:
- digit addition by module-two;
- digit addition module-two with correction;

2) module four additon:
- left-handed module four addition;
- right handed module four addition.

The transposition of elementary functions in operations does not affect the number of modified groups of operations with a transposition accuracy. The only operation that implements the encoding of a bit of information regardless of the serial number of the bit is the digit addition by module two. Based on this we can define the following list of operations:

1) module-two additon:
- digit addition by module-two:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} \qquad (5)$$

- digit addition module-two with correction;

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix} \qquad (6)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \oplus x_3)\cdot(k_1 \oplus k_3) \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \oplus (x_2 \oplus x_3)\cdot(k_2 \oplus k_3) \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \oplus (x_2 \oplus x_3)\cdot(k_2 \oplus k_3) \end{bmatrix}$$

2) module four additon:
- left-handed module four addition:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \cdot k_2 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \cdot k_3 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix};$$

- right handed module four addition:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_1 \cdot k_1 \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix};$$

3) module eight additon:
- left-handed module eight addition;

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_3 \cdot k_3 \vee k_2 \cdot x_3 \cdot k_3) \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_3 \cdot k_3 \vee x_3 \cdot x_2 \cdot k_2 \vee k_3 \cdot x_2 \cdot k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix}$$

- right handed module eight addition.

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_1 \cdot k_1 \vee k_2 \cdot x_1 \cdot k_1) \end{bmatrix} O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_1 \cdot k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \cdot k_1 \vee x_1 \cdot x_2 \cdot k_2 \vee k_1 \cdot x_2 \cdot k_2) \end{bmatrix}.$$

The given operations differ in mathematical representation and truth tables of transactions. Generalized tables of transactions with permutation accuracy also differ. Based on this, at least 14 groups of symmetric double-operand operations of cryptographic information coding for block encryption systems will be constructed based on the proposed synthesis method.

Let's synthesize basic group of symmetric three-digit double-operand matrix operations of cryptographic coding based on operation (6). For this purpose, we introduce a substitution in the operation

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

$$y_1 = x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2);$$

$$y_2 = x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2);\ y_3 = x_3 \oplus k_3$$

Using the basic three-digit single-operand matrix operations shown in table 1, we obtain 28 basic three-digit single-operand matrix operations:

$$O_1 = F_1(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_2 = F_2(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_3 = F_3(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_4 = F_4(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

$$O_5 = F_5(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_6 = F_6(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_7 = F_7(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_8 = F_8(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_9 = F_9(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{10} = F_{10}(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{11} = F_{11}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{12} = F_{12}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{13} = F_{13}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \end{bmatrix};$$

$$O_{14} = F_{14}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{15} = F_{15}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{16} = F_{16}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_1 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{17} = F_{17}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$O_{18} = F_{18}(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{19} = F_{19}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{20} = F_{20}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{21} = F_{21}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{22} = F_{22}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \end{bmatrix};$$

$$O_{23} = F_{23}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{24} = F_{24}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{25} = F_{25}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{26} = F_{26}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{27} = F_{27}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{28} = F_{28}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2)\cdot(k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix}.$$

To verify the correctness of the results of the synthesis of the obtained symmetric matrix operations, the requirements to the symmetry of the transactions given by the truth tables were applied. Additionally, each operation was verified by taking into account the complete enumeration of all input data.

Similarly, groups of symmetric double-operand operations based on an operation by using both a complete group of three-digit single-operand matrix operations and groups of three-digit single-operand nonlinear operations were synthesized. When constructing symmetric double-operand operations based on nonlinear three-digit single-operand nonlinear operations, it was found that the complexity of the models increased. This complication is related to the necessity of transition from representation of discrete models based on addition by module two to representation of discrete models in the basis of "AND-OR-NET"

During the process of implementation the method of synthesis the groups of symmetric double-operand

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

operations of cryptographic coding of information was found the following:

- based on each selected three-digit double-operand operation according to (3) 6 permutation operations will be constructed [17]. By applying the inversion of elementary functions, 8 inversion operations will be constructed of each obtained operation [17]. This will make it possible to extract 48 modifications of this operation from one symmetric three-digit double-operand operation, each of which is suitable for constructing a group of operations based on it.;
- the application of the proposed method of synthesis of groups of symmetric double-operand operations of cryptographic coding information for block coding systems based on one symmetric double-operand operation by using 28 three-digit basic matrix operations [17] will provide the construction of a group of 28 symmetric double-operand operations. The use of 48 modifications of the symmetric double-operand operation will provide the construction of 48 groups of operations, including 1344 symmetric three-digit double-operand matrix operations.;
- since the total number of three-digit single-operand matrix operations includes 1344 operations [17], then based on one symmetric three-digit double-operand operation will be built 64512 symmetric three-digit double-operand matrix operations.
- the maximum number of synthesized symmetric three-digit double-operand operations based on one given operation will be 1935360 operations since the full group of three-digit single-operand operations is 40320 (but their formalization is complicated by the absence of a single mathematical apparatus describing the whole set of linear and nonlinear single-operand operations). the maximum number of synthesized symmetric three-digit double-operand operations based on one given operation will be 1935360 operations since the full group of three-digit single-operand operations is 40320 (but their formalization is complicated by the absence of a single mathematical apparatus describing the whole set of linear and nonlinear single-operand operations)..
- when implementing the method of synthesis of groups of symmetric double-operand operations of cryptographic coding information in automated intelligent design systems, it is reasonable to represent crypto-transformation operations as mathematical models and truth tables to build in knowledge and data bases.

The application of the technology of building groups of symmetric matrix operations is not limited to the synthesis of groups of two- and three-digit operations. The obtained results allow to considerably expand both possibilities of developers of "lightweight cryptography" and variability of synthesized crypto-algorithms. Simplicity of realization of the offered method of symmetric matrix operations allows to use it for construction and filling of knowledge and data bases of intellectual systems of cryptoalgorithms designing. To ensure the speed of implementation of multi-digit double-operand nonlinear symmetric crypto-transformation operations it is reasonable to use substitution tables, the implementation of which compensates the lack of mathematical apparatus of formalized description of operation models.

Conclusions

The proposed method of synthesis of groups of symmetric double-operand operations of information cryptographic coding provides an opportunity to increase the variability of lightweight cryptoalgorithms by increasing significantly the total number of used operations. Additionally, the synthesis of symmetric cryptographic coding operations belonging to different mathematical groups provides increased crypto stability of the algorithm. Application of the double-operand cryptographic coding operations, to which the synthesized operations belong, leads to an insignificant increase in the complexity associated with implementation of synthesis of operations both at the hardware and software levels.

In the process of implementation of the method of synthesis of groups of symmetric double-operand operations of cryptographic coding of information it was found that on the basis of the known symmetric three-bit double-operand cryptographic conversion operation it is possible to build up to 1935360 its modifications with similar possibilities of use in crypto algorithms. This result allows to increase by an order of magnitude the variability of information protection algorithms.

Further research of the presented topic was expedient to conduct on three-operand, and later on multi-operand operations. However, the received results are suitable for practical use in developing new block encryption systems with increased speed and reliability of cryptographic transformation of information or, for example, in improving generation of pseudorandom sequences.

References

1. Horbenko, I. D., Horbenko, Yu. I. (2012), *Applied cryptology: monograph* [*Prykladna kryptolohiia: monohrafiia*], Kharkiv: Kharkiv National University of Radio Electronics, LLC "Fort", 868 p.
2. Bevz, O. M., Kvєtnii, R. N. (2010), *Data Encryption Based on Highly Nonlinear Boolean Functions and Maximum Distance Codes:* monograph [*Shyfruvannia danykh na osnovi vysoko neliniinykh bulevykh funktsii ta kodiv z maksymalnoiu vidstanniu*: monohrafiia], Vinnytsia: Vinnytsia National University of Technology, 96 p.
3. Manifavas, C., Hatzivasilis, G., Fysarakis, K., Rantos, K. (2012), "Lightweight cryptography for embedded systems a comparative analysis", *In: 6th International Workshop on Autonomous and Spontaneous Security SETOP 2012, Springer, LNCS, 8247,* P. 333–349. **DOI:** https://doi.org/10.1007/978-3-642-54568-9_21
4. Gildas Avoine, Julio Hernandez-Castro (2021), "Security of Ubiquitous Computing Systems", *Selected Topics. Springer,* P. 265 **DOI:** https://doi.org/10.1007/978-3-030-10591-4
5. Biryukov Alex and Perrin Leo (2017), "State of the art in lightweight symmetric cryptography", *Cryptology ePrint Archive, Report 2017/511,* available at: http://eprint.iacr.org/2017/511, https://eprint.iacr.org/2017/511.pdf

6. Mitsuru Matsui (1997), "New block encryption algorithm MISTYC", *In Eli Biham, editor, Fast Software Encryption – FSE'97, pringer, volume 1267 of Lecture Notes in Computer Science, Haifa, Israel, January 20–22,* P. 54–68, available at: https://link.springer.com/chapter/10.1007/BFb0052334
7. Hatzivasilis George, Fysarakis Konstantinos, Ioannis (2018), "Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers", *Cryptographic Engineering,* No. 8 (2), P. 141–184. **DOI:** https://doi.org/10.1007/s13389-017-0160-y
8. Kerry A. McKay, Larry Bassham, Meltem Sonmez Turan, and Nicky Mouha (2016), "Nistir 8114 - report on lightweight cryptography". **DOI:** https://doi.org/10.6028/NIST.IR.8114
9. Rudnytsky, V. M., Lada, N. V., Babenko, V. G. (2018), *Cryptographic coding: synthesis of stream encryption operations with accuracy to permutation: monograph* [*Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovky: monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 184 p.
10. Rudnitsky, V. M., Milchevich, V. Ya., Babenko, V. G., Melnyk, R. P., Rudnitsky, S. V., Melnyk O. G. (2014), *Cryptographic coding: methods and means of implementation (part 2):* monograph [*Kriptograficheskoe kodirovanie: metody i sredstva realizacii (chast' 2):* monografiya], Monograph, Kharkov: Publishing house "Shchedra sadyba plius", 223p.
11. Rudnytsky, V. M., ed. (2018), *Cryptographic coding: information processing and protection: collective monograph* [*Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kolektyvna monohrafiia*], Monograph, Kharkiv: LLC "DISA PLUS", 139p.
12. Sysoienko, S., Myronets, I., Babenko, V. (2019), "Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation", *Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), CEUR Workshop Proceedings 2353, CEUR-WS.org,* P. 402–412. (Scopus) available at: http://ceur-ws.org/Vol-2353/, http://ceur-ws.org/Vol-2353/paper32.pdf
13. Rudnitsky, V., Berdibayev, R., Breus, R., Lada, N. and Pustovit, M. (2019), "Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation", *Advanced Information Systems, Kharkiv: NTU "KhPI",* No. 3 (4), P. 109–114. **DOI:** http://doi.org/10.20998/2522-9052.2019.4.16
14. Lada, N. V., Kozlovska, S. G., Rudnitsky, S. V. (2019), " The symmetric operations' mathematical group constructing based on module-2 addition " ["Pobudova matematy`chnoyi grupy` sy`metry`chny`x operacij na osnovi dodavannya za modulem dva"]. *Modern special technics: scientific and practical journal. Kyiv,* No 4 (59), P.33–41.
15. Lada, N. V., Kozlovska, S. G. and Rudnitskaya, Y. V. (2019), "Researching and Synthesizing a Group of Symmetric Modified Modulo-4 Addition Operations" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii dodavannia za modulem chotyry "], *Central Ukrainian Scientific Bulletin. Technical Sciences,* No. 2 (33), P. 181–189. **DOI:** http://doi.org/10.32515/2664-262x. 2019.2(33)
16. Lada, N. V., Rudnitsky, S. V., Zazhoma, V. M. and Rudnytska, Y. V. (2020), " Research and synthesis of a group of symmetric modified operations of right-handed addition by module four" ["Doslidzhennia i syntez hrupy symetrychnykh modyfikovanykh operatsii pravostoronnoho dodavannia za modulem chotyry"], *Control, Navigation and Communication Systems. Academic Journal. Poltava: PNTU,* No. 1 (59), P. 93–96. **DOI:** https://doi.org/10.26906/SUNZ.2020.1.093
17. Rudnitsky, V. M., Babenko, V. G., Rudnitsky, S. V. (2012), " Method of synthesis of matrix models of operations of cryptographic recoding of information" ["Metod syntezu matrychnykh modelei operatsii kryptohrafichnoho perekoduvannia informatsii"], *Ukrainian Information Security Research Journal,* Vol 14, No. 3 (56), P. 50–56. **DOI:** https://doi.org/10.18372/2410-7840.14.3360

Received 18.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Лада Наталія Володимирівна – кандидат технічних наук, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, м. Черкаси, Україна; e-mail:Ladanatali256@gmail.com; ORCID: https://orcid.org/0000-0002-7682-2970

Lada Nataliia – Candidate of Technical Sciences, Associate Professor of Department of Information Security and Computer Engineering Cherkasy State Technological University, Cherkasy, Ukraine.

Лада Наталия Владимировна – кандидат технических наук, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, г. Черкассы, Украина.

Рудницька Юлія Володимирівна – аспірант (PhD) кафедри інформаційних технологій проектування Черкаського державного технологічного університету, м. Черкаси, Україна; e-mail: U.V.Rudnitskaya@gmail.com; ORCID: https://orcid.org/0000-0001-6384-0523

Рудницкая Юлия Владимировна – аспирант (PhD) кафедры информационных технологий проектирования Черкасского государственного технологического университета, г. Черкассы, Украина.

Rudnytska Yuliia – PhD of Department of Information Technology Design Cherkasy State Technological University, Cherkasy, Ukraine.

РЕАЛІЗАЦІЯ МЕТОДУ СИНТЕЗУ ГРУП СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ІНФОРМАЦІЇ ДЛЯ СИСТЕМ БЛОКОВОГО ШИФРУВАННЯ

Об'єктом дослідження є процеси побудови груп симетричних двохоперандних операцій криптографічного кодування інформації. **Предметом** дослідження є особливості реалізації узагальненого методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для «полегшеної криптографії». **Мета** роботи – дослідити процес побудови і реалізації методу синтезу груп симетричних багаторозрядних двооперандних операцій криптографічного

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

кодування інформації для забезпечення автоматизації пошуку шляхів збільшення варіативності і стійкості полегшених криптоалгоритмів. В статті вирішуються наступні **завдання:** визначити математичну групу однооперандних операцій на основі якої буде представлено реалізацію методу синтезу груп симетричних двохоперандних операцій криптографічного кодування; запропонувати технологію пошуку симетричних двохоперандних операцій; оцінити потужність синтезованих груп операцій та їх вплив на варіативність та стійкість алгоритмів «полегшеної криптографії». Отримано наступні **результати:** запропоновано технологію визначення симетричних двохоперандних операцій які будуть основою для синтезу групи симетричних двохоперандних операцій; запропоновано та реалізовано метод синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування; на прикладі порозрядного додавання за модулем два з корекцією та використання трьохрозрядних однооперандних операцій показано практичну реалізацію даного методу; на основі синтезованих операцій та наведених кількісних характеристики множини однооперандних операцій проведено оцінку потужностість синтезованих груп операцій та їх вплив на варіативність та стійкість алгоритмів «полегшеної криптографії». **Висновки:** запропонований то реалізований метод синтезу груп симетричних двооперандних операцій криптографічного кодування інформації дозволяє забезпечити можливість збільшення варіативності полегшених криптоалгоритмів. Синтез симетричних операцій криптографічного кодування, що належать різним математичним групам, забезпечує підвищення криптостійкість алгоритму. Застосування синтезованих операцій криптографічного кодування, приводить до значного збільшення варіативності криптоалгоритмів та їх складності.

Ключові слова: криптографічне кодування; полегшена криптографія; синтез груп симетричних операцій.

РЕАЛИЗАЦИЯ МЕТОДА СИНТЕЗА ГРУПП СИМЕТРИЧЕСКИХ ДВУХОПЕРАНДНЫХ ОПЕРАЦИЙ КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ ИНФОРМАЦИИ ДЛЯ СИСТЕМ БЛОЧНОГО ШИФРОВАНИЯ

Объектом исследования есть процессы построения групп симметричных двухоперандных операций криптографического кодирования информации. **Предметом** исследования есть особенности реализации обобщенного метода синтеза групп симметричных двухоперандных операций криптографического кодирования информации для «облегченной криптографии». **Цель** работы – исследовать процесс построения и реализации метода синтеза групп симметричных многоразрядных двухоперандных операций криптографического кодирования информации для обеспечения автоматизации поиска путей увеличения вариативности, и устойчивости облегченных криптоалгоритмов. В статье решаются следующие **задачи:** определить математическую группу однооперандных операций, на основе которой будет представлена реализация метода синтеза групп симметричных двухоперандных операций криптографического кодирования; предложить технологию поиска симметричных двухоперандных операций; оценить мощность синтезированных групп операций, и их влияние на вариативность и устойчивость алгоритмов "облегченной криптографии". Получены следующие **результаты:** предложена технология определения симметричных двухоперандных операций, которые будут основой для синтеза группы симметричных двухоперандных операций; предложен и реализован метод синтеза групп симметричных двухоперандных операций криптографического кодирования информации для систем блочного шифрования; на примере поразрядного сложения по модулю два с коррекцией, и использования трехразрядных однооперандных операций показана практическая реализация данного метода; на основе синтезированных операций и приведенных количественных характеристик множества однооперандных операций проведена оценка мощности синтезированных групп операций и их влияние на вариативность и стойкость алгоритмов «облегченной криптографии». **Выводы:** предложенный и реализованный метод синтеза групп симметричных двухоперандных операций криптографического кодирования информации позволяет обеспечить возможность увеличения вариативности облегченных криптоалгоритмов. Синтез симметричных операций криптографического кодирования, принадлежащих разным математическим группам, обеспечивает повышение криптостойкости алгоритма. Применение синтезированных операций криптографического кодирования приводит к значительному увеличению вариативности криптоалгоритмов и их сложности.

Ключевые слова: криптографическая кодировка; облегченная криптография; синтез групп симметричных операций.

Бібліографічні описи / Bibliographic descriptions

Лада Н. В., Рудницька Ю. В. Реалізація методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 35–43. DOI: https://doi.org/10.30837/ITSSI.2022.20.035

Lada, N., Rudnytska, Y. (2022), "Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 35–43. DOI: https://doi.org/10.30837/ITSSI.2022.20.035

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 061.3:378 DOI: https://doi.org/10.30837/ITSSI.2022.20.044

D. LYTVYNENKO, O. MALYEYEVA

RISK MANAGEMENT IN PROJECTS OF RESTORATION THE REGIONAL TRANSPORT STRUCTURE ON THE BASIS OF PARTICIPANTS' COMMUNICATION

The **subject** of the article is the processes of risk management and project communications. The components of the content of transport infrastructure rehabilitation projects, including communications between stakeholders, are considered. The **aim** of the work is to develop a method for assessing and managing the risks in transport infrastructure rehabilitation projects, taking into account the communication processes of the participants. The following **tasks** are solved in the article: systematization of risks in transport infrastructure rehabilitation projects in the form of relations between the project participants, creation of a graphic scheme of stakeholder communications, formalization of stakeholder communications with regard to the causes and possible parry of risks, development of a quantitative assessment model of the project risks with regard to stakeholder interests. **Methods** used: project management methodology, stakeholder theory, value theory, systems approach, matrix models. The following **results** were obtained: Opportunities, impact and risk status in relation to stakeholders of the transport infrastructure rehabilitation project were analyzed. The possibility of grouping risks in relation to the stakeholders of the project and the possibility of influence of stakeholder interaction on the available risk groups were considered. The risks that can directly affect the project or be affected by the interaction between the project stakeholders were identified. The formalized representation of risks and communications of project participants is presented. Opportunities to optimize the process of project risk management through the management of stakeholders and project communications have been identified. Quantitative project risk value model was developed to assess the effectiveness of actions to parry risks from stakeholders. **Conclusions:** project risk management can be more effective if tools and methods specific to stakeholder management and project communications are applied. The proposed formalization establishes a clear model of stakeholder interaction to parry risks. The model of quantitative assessment of the effectiveness of actions to parry risks will allow to evaluate the effectiveness of the management strategy and to make adjustments in time. In the future, this work will continue scientific research in the direction of developing models and methods of research of communications and risks of the project

Keywords: project management; stakeholders; transport infrastructure; interaction model; risk assessment.

Introduction

Success in the implementation of complex projects is associated with considerable uncertainty in the various factors accompanying the project. For example, the timing of the decision on financing and obtaining the result may not be too certain, although it is almost a key factor for every project.

As a result of the large-scale aggression of the Russian Federation in 2022, Ukraine suffers significant losses in the condition, quality and overall suitability of infrastructure facilities of entire regions. As of June 2022, the Ministry of Infrastructure sounded Ukrainian losses at 20-30% of prewar capabilities [1]. The scale of the damage varies from region to region and is not final, but it is already obvious that the country is waiting for a huge scale of projects to restore the lost infrastructure.

The specifics of transportation infrastructure rehabilitation projects include the involvement of significant financial resources, which may not be possible with significant schedule and outcome volatility. Failure to fully assess and account for all project risks can lead to significant and sometimes critical consequences, such as project non-completion or reduced overall benefits. This makes the field of risk management extremely critical and important to both project management and transportation system development projects in particular. After all, long-term and financially costly projects are particularly affected by a dynamic and uncertain environment [1].

The need to increase investment activity requires modern science to develop models and tools to qualitatively and reliably perform the tasks and carry out preventive measures to reduce the impact of project risks. Risk management is an effective tool for regulating changes in the economic environment[2].

Analysis of recent research and publications

A significant contribution to the domestic science in the field of research and development of methods and tools of risk management was made by such scientists as Bushuyev S.D. [3], Rach V.A., Zyuzyun V.O. [4], Druzhinin E.A. and others.

Risk assessment plays a key role in the management process. It may be done by economic, mathematical, statistical methods, by the method of expert evaluations or by a combined method. The main indicators, on the basis of which the mathematical and statistical assessment takes place, are the coefficient of variation and the degree of risk.

Rach V.A. showed the significance and difference of risks depending on the sphere and phase of the project, in which they can occur. Thus, according to the scientist, risks can be characterized by industry depending on the life cycle of the project and relative to the stakeholders of the project. He proposed the use of the risk pyramid and built a model that allows managers to effectively carry out risk management [5].

Druzhinin E.A. proposed the concept, principles and system scenario of the risk-oriented approach in project resource management. The scientist proposes to take into account the impact of the manifestation of multiple external and internal risks to justify the resources by joint modeling of project actions and actions aimed at eliminating the consequences of risk manifestation, which ensures the sustainability of the ongoing projects [6].

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Latkin M.O. proposes to use a system approach to describe risk management as a hierarchical system; including structural models (target model, functional model, organizational structure model) and process, models (process model of the implementation of management functions and communication model). The interaction between the individual models of the risk management system is provided by a number of matrix projections [7].

Foreign publications increasingly pay attention to current trends and the possibilities of their impact on the field of project management, in particular, risk management and communication. Wilson and co-authors investigated the possibilities of applying the value-based approach in risk management [8] and the possibilities of applying artificial intelligence for more effective risk management and communication in the project [9]. In recent years, scientists often address the topic of COVID-19 and its impact on the industry [10 - 12]. To date, it is relevant to study the risks of projects in supercomplicated critical conditions, such as wartime and post-war period.

The analysis of publications on risk management showed that the industry remains dynamic and attempts to describe processes and create tools continue with different approaches and tools. This indicates an incomplete process of basic knowledge and research methods, i.e., the development and search for new models must continue. It has also been determined that quite rarely the scientists pay attention to the branch specificity of the project and often do not adapt the resulting research tools to emergency conditions and challenges. Consequently, there is a need for closer integration of existing models into the current modern conditions and needs of the industry, for example, so important for the country and regions as the transport industry.

At the same time, the impact of communication technologies and communication management techniques as a means of risk management remains little explored. Popular methodologies in communication management and risk management refer to different areas of knowledge and rarely mention their relationship [13]. Although the setting up and streamlining of communication processes affects not only the awareness of project participants, but also their trust in each other and, accordingly, affects the reliability of decisions and risks of the project.

Highlighting the previously unresolved parts of the general problem. Purpose of the work

The purpose of the presented research is to develop a method for assessing and managing risks in transport infrastructure restoration projects, taking into account communication processes. The results should become a reliable tool for applying in practice and solving the problems of risk management strategies.

The article addresses the following objectives:

1. Systematization of risks in transport infrastructure rehabilitation projects through relationships between project participants.

2. Creating a graphic diagram of stakeholder communications.

3. Formalization of stakeholder communication processes, taking into account the causes and possible parry of risks.

4. Development of a model for quantitative assessment of project risks, taking into account the interests of stakeholders.

Main results of the study

The transport infrastructure is an integral part of the system in which it exists. It can be either the transport infrastructure of a country or a separate settlement within the framework of their own infrastructures and needs. The transport infrastructure reconstruction project has a number of differences in the life cycle of the project. Indeed, the preparatory stage plays a significant role. To avoid significant risks, there must be an assessment of the impact of the implementation process on the environment, on the interests of local residents, authorities, stable use and permanence, which may be critical and necessary. Also, a detailed study requires the logistical capacity of the region and the ability to manufacture and deliver the necessary construction materials, equipment and all necessary human resources must be quickly available. The financial component of the project should be balanced and work effectively throughout the duration of the project. During the work, special attention should be focused on safety issues, both for the population and workers, as well as the ecological systems of the region. Clear and effective management of communication between stakeholders will allow rapid and effective adaptation to critical conditions throughout the life cycle of the project.

Based on the analysis of possible stakeholders of transport infrastructure rehabilitation projects [15], the analysis of methods of applying the value-based approach, the analysis of modern methods of stakeholder management, each stakeholder may have its own interests, goals, expectations and risks in relation to the project [16]. Accordingly, the risks may have a different impact, assessment and status in relation to the stakeholder, as well as in relation to the stage of the project life cycle. Accounting for such risks, their control and management is an important part of the project manager's work, and sometimes a critical part of the work, because the most critical risks and their inadequate management can threaten the existence of the project as a whole.

Based on the analysis of the interaction between the stakeholders of the transport infrastructure rehabilitation project [17], all project stakeholders can be divided and grouped as follows: the project team, project executors, project suppliers, investors, authorities and society. Each of these stakeholder groups may have both internal risks that depend more on the internal processes of the stakeholder group itself, and external risks that determine the interrelated expectations of opportunities and problems of one stakeholder group in regard to others.

Risk management is defined as a set of tools, methods, forms and means of interaction of subjects of

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

risk management in order to develop and implement management decisions aimed at preventing the risks of investment activities, reducing and overcoming the effects of its impact [14].

Risk management involves:

- the use of all possible means in order to avoid or reduce the degree of risk associated with significant losses;
- controlling risk in case it cannot be avoided completely;
- optimization of risk degree or reduction of probable losses;
- conscious acceptance of risk and preparation of all possible processes triggered by this risk.

According to the PMBOK methodology [13], risk management is divided into stages: planning, identification, qualitative analysis, quantitative analysis, response planning, and monitoring. Each of these procedures is performed at least once in each project. In spite of the fact that developers of the standard clearly separate these procedures, in practice they often can be implemented in a unified procedure, coincide and closely cooperate.

The grouping of risks and their representation by means of relations between participants of the project was offered in works Gritsenko L.L. [18]. In this paper, the groups of risks are expanded on the example of the outlined groups of stakeholders of transport infrastructure rehabilitation projects.

In the risk system, we can distinguish the groups of risks containing individual partial risks. In addition, partial risks to the project participant may be caused by another participant.

So, for example, for the performer of works and society in relation to the state there are the following groups of risks:

- political risks (change of power, change of officials, decline in political will, political crises);
- excessive influence of the state in the project (bureaucratic obstacles, corruption component, pressure of controlling bodies)
- financial risks (shortage and stoppage of funding, failure to fulfill assigned obligations, inability to fulfill promised simplifications and benefits).

Authorities and investors have the following partial risks in relation to performers:

- technical errors and low level of preparatory work;
- irrational chosen form of contract and partnership;
- poor quality of work; mistakes in the execution of works;
- unscrupulousness and outright fraud on the part of producers of works.

The following partial risks are possible for the authorities and executors in relation to the society:

- risks of protest sentiments in society;
- risks of public ignorance and failure to understand the value of the project.

The society may experience the following partial risks in relation to the government and the executor:

- risks of deterioration of the ecological condition of the region;
- risks of destruction and deformation of the usual way of life, places of habitation;
- the low quality of the obtained infrastructure.

The supplier group is one of the most isolated and primarily dependent on proper financing from the work producer, and the work producer, accordingly, will risk receiving equipment and goods of inadequate quality and with delays.

Table 1 shows the interrelation of groups of project participants because of their respective risks. The table does not reflect the project team, because they are interested in reducing the probability of each risk and interact with every other project participant [16]. The table is not exhaustive and complete, but can serve as an illustration of the relationship between project participants on the basis of risks.

Table 1. *Scheme of stakeholder communications, taking into account the causes and possible parrying of risks*

Project stakeholder	***Partial risks***	***Stakeholders interested in parrying partial risks***
Contractor (S_1)	Low level of preparatory work (r_1)	Authorities, investor
	Errors in the contract (r_2)	Authorities, investor
	Poor quality of work performance (r_3)	Authorities, society
	Unfairness and outright fraud (r_4)	Authorities, community, investor, suppliers
	Financial instability (r_5)	Authorities, community, investor, suppliers
	Non-compliance with environmental, moral standards (r_6)	Authorities, society
	Lack of attention to the environment, community sustainability, and historicity (r_7)	Authorities, society
Project provider (S_2)	Inadequate quality of goods and equipment (r_8)	The executor
	Problems with supply timing (r_9)	Executor
Investor (S_3)	Inadequate financial performance (r_{10})	Authorities, executor
Authorities (S_4)	Political instability in the region (r_{11})	Investor, society, executor
	Bureaucracy and excessive control (r_{12})	Performer, Supplier
	Financial instability in the region (r_{13})	Executor, investor
Society (S_5)	Protest sentiment (r_{14})	Authorities, executor
	Lack of awareness (r_{15})	Authorities

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

On the basis of this table it is possible to graphically depict the scheme of stakeholder communications, taking into account the causes and possible parry of risks (fig. 1). In the figure in the zones of the corresponding stakeholder the partial risks that can be caused by it are indicated. Arrows show stakeholder communications on the parrying of risks (or their group). The direction of the arrow indicates which stakeholder is interested in parrying the relevant risks (start) caused by another stakeholder (end).

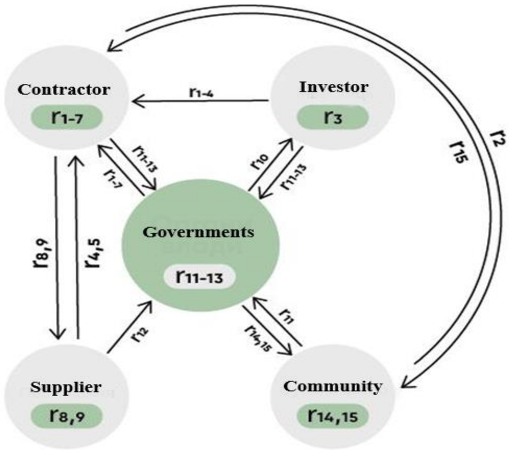


Fig. 1. Scheme of stakeholder communications, taking into account the causes and possible parrying of risks

It should be noted that such a relationship of certain stakeholders is typical, and has been noted in studies devoted to stakeholder management at the stages of the project life cycle [19].

For the formalized representation of risks and communications of participants, we introduce the following notations.

Partial risks constitute the set $R = \{r_k\}$, k = 1..m. Project stakeholders constitute the set $S = \{S_i\}$, i = 1..n.

Stakeholder S_i is interested in reducing the risks caused by stakeholder S_j. We denote this subset of risks by R_{ij},

$$R_{ij} \subset R .$$

Using the above designations, the generalized matrix of the relationship between stakeholders on risk-pairedness is presented in table 2.

Table 2. *Generalized matrix of interrelations between stakeholders on the parrying of risks*

	S_1	…	S_j	…	S_n
S_1	-	…	R_{1j}	…	R_{1n}
…	…	…	…	…	…
S_i	R_{i1}	…	R_{ij}	…	R_{in}
…	…	…	…	…	…
S_n	R_{n1}	…	R_{nj}	…	-

Risk management can be considered not only in the context of risk per se, but also in the context of stakeholder management and communication management, including between stakeholders. Building clear and transparent communication processes can not only reduce risk, but also build a robust system of trust between project members (fig. 2).

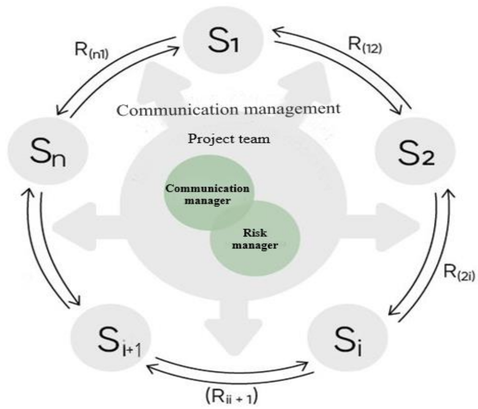


Fig. 2. Generalized model of project stakeholder communications management in order to reduce risks

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

To achieve these goals, reliable and regular communication must be built between the party bearing the risk and the party for whom the occurrence of this risk is critical and important. For example, reducing the probability of the risk of "low level of preparatory work" can be ensured by effectively informing the parties both on the part of the contractor about the progress of such work, and on the part of the authorities by controlling and ensuring clear and transparent rules and standards for the performance of work. Or the reduction of the likelihood of protest sentiments among the population is achieved through an open and regular dialogue between the population (representatives of initiative groups, public organizations, etc.) and the authorities or the contractor. The population must also be informed through the media, social networks, advertisements or other means of disseminating information about the project, its safety, necessity and value.

Thus, the management of each risk requires additional standardization and can cause excessive bureaucracy. In order to reduce the risk of project bureaucracy, it is suggested that information technology be used extensively to reduce routine processes and automate control of communication and document exchange.

In order to quantify the possible risks caused by project stakeholders at different stages of the project life cycle, the following parameters should be considered: p_k - the probability of partial risk r_k; d_k - the possible losses of the project caused by risk r_k, $k = 1..m$.

The probability of risk is assessed by expert methods or by a decision maker - risk manager.

Possible losses of the project are expressed in a cost degree (although it can be the cost of time or a decrease in the quality of work performed).

The negative impact of partial risks on the main indicators of the project is shown in table 3.

Table 3. *Impact of partial risks on the main parameters of the project*

Partial risks	***Main parameters of the project***		
	Cost	***Duration***	***Quality of work***
Low level of preparatory work (r_1)		+	+
Errors in the contract (r_2)	+	+	+
Poor quality of work performance (r_3)			+
Unfairness and outright fraud (r_4)	+	+	+
Military instability (r_5)	+		
Non-compliance with environmental, moral standards (r_6)			+
Lack of attention to the environment, community sustainability, and historicity (r_7)			+
Inadequate quality of goods and equipment (r_8)			+
Problems with supply timing (r_9)		+	
Inadequate financial performance (r_{10})	+		
Political instability in the region (r_{11})	+	+	
Bureaucracy and excessive control (r_{12})	+	+	
Financial instability in the region ((r_{13})	+		
Protest sentiment (r_{14})		+	
Lack of awareness (r_{15})	+	+	

To quantify the effectiveness of actions to parry risks from stakeholders, the following parameters should be considered [16]: *In* – interest (degree of interest) of a stakeholder in the project, *V* – degree of power (influence) on the project, *A* – resources (of different types), which the stakeholder has for participation in the project.

Let us denote the set of interests of separate stakeholder groups by $I = \{I_j\}$, $j = 1...mi$. The degree of interest of each stakeholder is measured by x_{ij}, in the general case $x_{ij} \in [-1,1]$, $i = 1...n$, $j = 1...mi$. Note that due to the method of harmonization of interests with project goals, a set of stakeholders is selected for which $x_{ij} > 0$ [20].

The total degree of interest of the i-th stakeholder in the project is defined as

$$In_i = \max\left(1, \sum_{j=1}^{mi} x_{ij}\right),$$

and only positive stakeholder interest is taken into account.

The set of stages of the life cycle (LC) of the project we denote as $E = \{e_l\}$, $l = 1..t$. Stakeholder influence coefficients on the project reflect the value of the matrix $K = \|k_{il}\|$, $i = 1..n$, $l = 1..t$, where k_{il} – level of influence of the *i*-th stakeholder at the *l*-stage of the project life cycle, *t* – number of stages of the project life cycle, $k_{il} \in [0,1]$.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

Thus, it is possible to determine the probability of risk parrying rk by the *i*-th stakeholder at stage l of the life cycle as a function of

$$q_{ikl} = f\left(In_i, k_{il}\right)$$

under the conditions:

a) risk r_k belongs to the group of risks in which the *i*-th stakeholder is interested, i.e.

$$r_k \in R_i, R_i = \bigcup_j R_{ij} \quad ,$$

where R_i - groups of risks, in which *i*-th stakeholder is interested, includes all the risks that are the subject of communication with other stakeholders, which cause these risks,

б) risk r_k may occur at stage *l* of the life cycle.

Let us note that if risk r_k can occur at different stages of the life cycle, then the probability of its parrying by the *i*-th stakeholder is $q_{ik} = \min_l q_{ikl}$.

The quantitative assessment of risk r_k (possible losses for the project), taking into account its probability, is the product of $p_k d_k$.

Assessment of the necessary resources for its parry, taking into account the interest and power of stakeholders is $\sum_{j=1}^{n_k}(1-q_{ik})a_i$, where q_{ik} - probability of the *i*-th stakeholder to parry risk r_k , a_i - resources of the *i*-th stakeholder, represented in monetary form.

Thus, the reduction in the risk cost is

$$\Delta_k = p_k d_k - \sum_{i=1}^{n_k}(1-q_{ik})a_i .$$

If $\Delta k > 0$, then the risk remains and management decisions must be made to increase the intensity of communication between the stakeholder who is the cause of the *k*-th risk and many interested stakeholders, or to attract additional (insurance) resources to the project.

Conclusions and prospects for further development

Consideration of the main features of transport infrastructure reconstruction projects and their differences in relation to projects in other industries allowed to determine the range of stakeholders, taking into account the specifics of these projects.

The opportunities, impact and status of risks in relation to the stakeholders of transport infrastructure reconstruction project were analyzed. The systematization of risks in transport infrastructure reconstruction projects in the form of relationships between the project participants was carried out. The possibility of grouping risks in relation to the project stakeholders and the possibility of influence of stakeholder interaction on implicit groups of risks were deployed. A table and graphical schemes of the relationship between groups of project participants due to the relevant risks and methods of their parrying have been created.

Risks that may directly affect the project or be affected by interactions between project stakeholders are identified. A formalized representation of the risks and communications of project stakeholders has been provided. Opportunities to optimize the process of project risk management through the management of project stakeholders and communications have been identified. The model of quantitative assessment of the cost of risks of the project to assess the effectiveness of actions to parry the risks of stakeholders has been developed.

Scientific novelty is the improvement of the method of risk assessment and management in transport infrastructure reconstruction projects, which, unlike existing ones, is based on the systematization of risks, taking into account the interests and power of stakeholders and will assess the degree of risk and effectiveness of its parry based on the analysis of communication processes.

Thus, project risk management can be more effective when tools and methods specific to stakeholder management and project communications are applied. The proposed formalization establishes a clear model of stakeholder interaction for the parrying of risks. The model of quantitative assessment of the effectiveness of actions to parry risks will allow to evaluate the effectiveness of the management strategy and to make adjustments in time.

The developed method is an integral part of the information technology of risk management and communications of transport infrastructure reconstruction projects. In the future, this work will allow to continue scientific research in the direction of developing models and methods of research of communications and risks of the project.

References

1. Bashynska, I. O., Makarets, D. O. (2017), "Risk management in projects" ["Upravlinnya ryzykamy v proyektakh"], *Economy. Finances. Right*., No. 5 (2), P. 38–40.
2. Bashynska, I. O., Novak, N. G. (2017), "Effective management of enterprise projects" ["Efektyvne upravlinnya proyektamy pidpryyemstva"], *Market infrastructure*, No. 6, P. 113–117.
3. Bushuev, S. D., Bushuev, D. A. and Kozyr, B. Yu. (2019), "Change of paradigms in the management of infrastructure projects and programs" ["Zmina paradyhm v upravlinni infrastukturnymy proektamy i prohramamy"], *Management of development of complex systems*, No. 37, P. 6–12. **DOI:** https://doi.org/10.6084/m9.figshare.9783149
4. Zyuzyun, V. I. (2017), "Methods and models of environmental risk management in transport development projects" ["Metody ta modeli upravlinnya ekolohichnymy ryzykamy v proyektakh rozvytku transportu"]: dissertation, candidate technical Sciences: 05.13.22, Kyiv, 202 p.

5. Rach, V. A. (2013), "Danger/risk/crisis as a triadic essence of development processes in the modern economy" ["Nebezpeka/ryzyk/kryza yak triadna sutnist′ protsesiv rozvytku v suchasniy ekonomitsi"], *Project management and development of production*, No. 1, P. 155–160.
6. Druzhinin, E. A. (2014), "Mathematical support of information technology for the integration of processes in project planning, taking into account the influence of risk factors" ["Matematicheskoye obespecheniye informatsionnoy tekhnologii integratsii protsessov pri planirovanii proyektov s uchetom vliyaniya faktorov riska"], *Project management and development of production*, No. 2 (50), P. 42–48.
7. Latkin, M. A. (2014), "Management of reserves of time and cost in the performance of project work" ["Upravleniye rezervami vremeni i stoimosti pri vypolnenii rabot proyekta"], *Project management and development of production*, No. 2 (50), P. 107–118.
8. Wilson, H. J., Daugherty, P. R. (2018), "Collaborative intelligence: Humans and AI are joining forces", *Harvard Business Review*, No. 96 (4), P. 114 – 123.
9. Zerfass, A., Hagelstein, J. and Tench, R. (2020), "Artificial intelligence in communication management: a cross-national study on adoption and knowledge, impact, challenges and risks", *Journal of Communication Management*, Vol. 24 No. 4, P. 377–389. **DOI:** https://doi.org/10.1108/JCOM-10-2019-0137
10. Wong, C. M. L., Jensen, O. (2020), "The paradox of trust: perceived risk and public compliance during the COVID-19 pandemic in Singapore", *Journal of Risk Research*, 23:7-8, 1021-1030, **DOI:** https://doi.org/10.1080/13669877.2020.1756386
11. Karasneh, R., Al-Azzam, S., Muflih, S., Soudah, O., Hawamdeh, S. and Khader, Y. (2020), "Media's effect on shaping knowledge, awareness risk perceptions and communication practices of pandemic COVID-19 among pharmacists", *Res Social Adm Pharm.* Jan;17 (1):1897–1902. **DOI:** https://doi.org/10.1016/j.sapharm.2020.04.027.
12. Moreno, Á., Fuentes-Lara, C. and Navarro, C. (2020), "Covid-19 communication management in Spain: Exploring the effect of information-seeking behavior and message reception in public's evaluation", *Profesional de la información*, No. 29 (4). **DOI:** https://doi.org/10.3145/epi.2020.jul.02.
13. "Project management institute 2013 annual report", available at: http://www.pmi.org/ AboutUs/~/media/PDF/ Publica-tions/PMI-2013-Annual-Report-Web.ashx (last accessed 21.08.2021).
14. Tkach, S. M. (2015), "Risk management of investment activities in the region: theoretical foundations and applied aspects" ["Upravlinnya ryzykamy investytsiynoyi diyal′nosti v rehioni: teoretychni osnovy ta prykladni aspekty"]: monograph., Lviv: State University Institute of Regional Studies named after M. I. Dolishnyi National Academy of Sciences of Ukraine", 234 p.
15. Lytvynenko, D., Dorokhina, A. and Artiukh, R. (2019), "Analyzing the interests and interaction of the participants of a transport system development project", *Innovative Technologies and Scientific Solutions for Industries*, No. (7), P. 69–74. **DOI:** https://doi.org/10.30837/2522-9818.2019.7.069
16. Lytvynenko, D. P., Maleeva, O. V. (2020) "Stakeholder management models at the stages of the life cycle of transport system development projects" ["Modeli upravlinnya steykkholderamy na etapakh zhyttyevoho tsyklu proektiv rozvytku transportnykh system"], *Radioelectronic and computer systems*, No. 3, P. 97–107. **DOI:** https://doi.org/10.32620/reks.2020.3.10
17. Malyeyeva, O., Lytvynenko, D., Kosenko, V. and Artiukh, R. (2020), "Models of harmonization of interests and conflict resolution of project stakeholders", *ITPM 2020, Proceedings of the 1st International Workshop IT Project Management (ITPM 2020)*, Slavsko, Lviv region, Ukraine, February 18-20, CEUR Workshop Proceedings Vol-2565 http://ceur-ws.org/Vol-2565/paper3.pdf
18. Hrytsenko, L. L., Krasulya, T. Yu. (2011), "Risk management during the implementation of infrastructure projects within the framework of public-private partnership" ["Upravlinnya ryzykamy pry realizatsiyi infrastrukturnykh proektiv u ramkakh derzhavno-pryvatnoho partnerstva"], *Actual problems of the economy*, No. 12 (126), P. 85–90.
19. Lytvynenko, D., Malyeyeva, O. (2019), "A comprehensive method of balancing and harmonizing the interests of stakeholders in transport systems development projects", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (9), P. 91–98. **DOI:** https://doi.org/10.30837/2522-9818.2019.9.091

Received 24.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Литвиненко Дмитро Петрович – аспірант кафедри комп'ютерних наук та інформаційних технологій, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна, email: newboroshno@gmail.com. ORCID: 0000-0001-5766-0139.

Литвиненко Дмитрий Петрович – аспирант кафедры компьютерных наук и информационных технологий, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт», г. Харьков, Украина.

Lytvynenko Dmytro – graduate student of department of Computer science and information technology, National Aerospace University – "Kharkiv Aviation Institute" , NAU «KhAI», Kharkiv, Ukraine.

Малєєва Ольга Володимирівна – доктор технічних наук, професор, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», професор кафедри комп'ютерних наук та інформаційних технологій, м. Харків, Україна; e-mail: o.maleyeva@khai.edu; ORCID: 0000-0002-9336-4182.

Малеева Ольга Владимировна – доктор технических наук, профессор, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», профессор кафедры компьютерных наук и информационных технологий, г. Харьков, Украина.

Malyeyeva Olga – Doctor of Sciences (Technical Sciences), Professor, National Aerospace University "Kharkiv Aviation Institute"; Professor of the Department of Computer science and information technology, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

УПРАВЛІННЯ РИЗИКАМИ В ПРОЄКТАХ ВІДНОВЛЕННЯ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ РЕГІОНУ НА ОСНОВІ КОМУНІКАЦІЙ УЧАСНИКІВ

Предметом дослідження в статті є процеси управління ризиками та комунікаціями проєкту. Розглядаються складові змісту проєктів відновлення транспортної інфраструктури, зокрема комунікації між стейкхолдерами. **Мета** роботи – розробка методу оцінювання та управління ризиками у проєктах відновлення транспортної інфраструктури з урахуванням комунікаційних процесів учасників. В статті вирішуються наступні **завдання:** систематизація ризиків у проєктах відновлення транспортної інфраструктури у вигляді відношень між учасниками проєкту, створення графічної схеми комунікацій зацікавлених сторін, формалізація комунікації зацікавлених сторін з урахуванням причин та можливого парирування ризиків, розробка моделі кількісної оцінки вартості ризиків проєкту з урахуванням інтересів стейкхолдерів. Застосовані **методи:** методології управління проєктами, теорія стейкхолдерів, теорія цінностей, системний підхід, матричні моделі. Отримано наступні **результати:** Проаналізовано можливості, вплив та статус ризиків відносно стейкхолдерів проєкту відновлення транспортної інфраструктури. Розглянуто можливість групування ризиків відносно стейкхолдерів проєкту та можливості впливу взаємодії стейкхолдерів на наявні групи ризиків. Визначено ризики, що напряму можуть впливати на проєкт або піддаватися впливу взаємодії між стейкхолдерами проєкту. Надано формалізоване представлення ризиків та комунікацій учасників проєкту. Визначено можливості оптимізації процесу управління ризиками проєкту через управління стейкхолдерами та комунікаціями проєкту. Розроблено модель кількісної оцінки вартості ризиків проєкту для оцінювання ефективності дій з парирування ризиків зі сторони зацікавлених сторін. **Висновки:** управління ризиками проєкту може мати підвищену ефективність при застосування засобів та методів, характерних для управління стейкхолдерами та комунікаціями проєкту. Запропонована формалізація встановлює чітку модель взаємодії стейкхолдерів для парирування ризиків. Модель кількісної оцінки ефективності дій з парирування ризиків дозволить оцінити ефективність стратегії управління та вносити корективи вчасно. В подальшому, дана робота дозволить продовжити наукові дослідження в напрямку розробки моделей та методів дослідження комунікацій та ризиків проєкту.

Ключові слова: управління проєктами; стейкхолдери; транспортна інфраструктура; модель взаємодії; оцінка ризику.

УПРАВЛЕНИЕ РИСКАМИ В ПРОЕКТАХ ВОССТАНОВЛЕНИЯ ТРАНСПОРТНОЙ СТРУКТУРЫ РЕГИОНА НА ОСНОВЕ КОМУНИКАЦИЙ УЧАСНИКОВ

Предметом исследования в статье являются процессы управления рисками и коммуникациями проекта. Рассматриваются составляющие содержания проектов восстановления транспортной инфраструктуры, в том числе коммуникации между стейкхолдерами. **Цель** работы – разработка метода оценки и управления рисками в проектах восстановления транспортной инфраструктуры с учетом коммуникационных процессов участников. В статье решаются следующие **задачи:** систематизация рисков в проектах восстановления транспортной инфраструктуры в виде отношений между участниками проекта, создание графической схемы коммуникаций заинтересованных сторон, формализация коммуникаций заинтересованных сторон с учетом причин и возможного парирования рисков, разработка модели количественной оценки стоимости рисков проекта с учетом интересов стейколжеров. Применяемые методология управления проектами, теория стейкхолдеров, теория ценностей, системный подход, матричные модели **методы:**. Получены следующие **результаты:** Проанализированы возможности, влияние и статус риска в отношении стейкхолдеров проекта восстановления транспортной инфраструктуры. Рассмотрена возможность группирования рисков в отношении стейкхолдеров проекта и возможности влияния взаимодействия стейкхолдеров на имеющиеся группы рисков. Определены риски, которые могут напрямую влиять на проект или подвергаться влиянию взаимодействия между стейкхолдерами проекта. Представлено формализованное представление рисков и коммуникаций участников проекта. Определены возможности оптимизации процесса управления рисками проекта посредством управления стейкхолдерами и коммуникациями проекта. Разработана модель количественной оценки стоимости рисков проекта для оценки эффективности действий по парированию рисков со стороны заинтересованных сторон. **Выводы:** управление рисками проекта может иметь повышенную эффективность при применении средств и методов, характерных для управления стейкхолдерами и коммуникациями проекта. Предлагаемая формализация устанавливает четкую модель взаимодействия стейкхолдеров для парирования рисков. Модель количественной оценки эффективности действий по парированию рисков позволит оценить эффективность стратегии управления и вносить коррективы в срок. В дальнейшем данная работа позволит продолжить научные исследования в направлении разработки моделей и методов исследования коммуникаций и рисков проекта.

Ключевые слова: управление проектами; стейкхолдеры; транспортная инфраструктура; модель взаимодействия; оценка риска.

Бібліографічні описи / Bibliographic descriptions

Литвиненко Д. П., Малєєва О. В. Управління ризиками в проєктах відновлення транспортної інфраструктури регіону на основі комунікацій учасників. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 44–51. DOI: https://doi.org/10.30837/ITSSI.2022.20.044

Lytvynenko, D., Malyeyeva, O. (2022), "Risk management in projects of restoration the regional transport structure on the basis of participants' communication", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 44–51. DOI: https://doi.org/10.30837/ITSSI.2022.20.044

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 004.657; 004.051; 004.413.5 DOI: https://doi.org/10.30837/ITSSI.2022.20.052

O. MAZUROVA, I. SYVOLOVSKYI, O. SYVOLOVSKA

NOSQL DATABASE LOGIC DESIGN METHODS FOR MONGODB AND NEO4J

Modern developers of gaming mobile and Internet applications almost do not imagine themselves without the use of NoSQL databases, if they pursue the goal of creating scalable databases with high-performance and wide functionality. When designing a database for any NoSQL system, the developer needs a clear understanding of the logic of such databases and the capabilities of the tools offered by the corresponding DBMS. However, unfortunately, they do not have unified methods of logical design of such models, as in relational databases. Thus, there is a problem of developing effective methods for the logical design of such databases that would provide the necessary performance when implementing the business logic of the corresponding applications. The **subject** of the research is approaches to the logical design of NoSQL document and graph databases. The **goal** of the work is to propose unified logical modeling methods for MongoDB and Neo4j NoSQL systems based on an experimental study of their performance. The following tasks are solved in the work: analysis of current approaches to the logical design of document and graph databases\, the development of logical design methods for them; planning and experimental study of the performance of the proposed methods on the example of models developed with their help. The following **methods** are used: database design methods, database performance evaluation methods, development methods are based on MongoDB 5.0.5, Neo4j 4.4.3 DBMS, Visual Studio 2022 development environment. The following **results** are obtained: unified logical design methods for MongoDB and Neo4j NoSQL systems are proposed; on their basis, the corresponding logical models have been developed; experimental measurements of the number of resources required working with the developed models; recommendations on the proposed methods are formed. **Conclusions:** The proposed modeling methods for MongoDB have their own aspects of their effective use for different types of applications. The strengths and weaknesses of both methods were identified, but a mixed method based on a combination of modeling through normalization and denormalization was recommended. Even though Neo4j lost out to MongoDB in terms of consumed resources in most experiments, both DBMS's' demonstrate good productivity, taking into account the orientation to different tasks.

Keywords: database; logical design method; DB DESIGN; Neo4j; NoSQL; MongoDB.

Introduction

The amount of data on the Internet is growing at an enormous rate as active users add hundreds of gigabytes of data to social networks every second. Relational databases cannot cope with such modern masses of information, although data processing tasks have been successfully implemented for several decades.

This problem has led to the need to introduce new approaches to information processing in large systems. To date, NoSQL databases have met this challenge [1 - 2], which have made it possible to replace costly vertical scaling with efficient horizontal scaling on clusters. In addition, they have higher performance, more flexible data model, and open source DBMS code.

Now, the most popular NoSQL databases are document databases, in particular MongoDB, rapidly catching up with popular relational databases of Microsoft SQL Server, Oracle, MySQL and PostgreSQL [2]. In addition, when creating large systems, particularly for social networks, well proven graph DBMS, namely the most common DBMS Neo4j [3], which has a very wide functionality.

When designing a database for any NoSQL system, a developer is required to have a clear understanding of the logic of the database and the tools that DBMS offers [4]. Since this understanding may not happen in practice, many commercial projects hesitate to switch to new NoSQL databases, because the implementation of such a switch requires a lot of time for performance modeling and information migration.

Algorithms for transition from ER diagrams to logical models in the context of relational DB [5] have long been formalized. However, these algorithms are not applicable to NoSQL databases, which are based on data structures other than tables (relations).

Consequently, to solve the problem faced by developers of NoSQL databases, the task of developing more unified methods of logical modeling of such databases and their experimental study in order to identify more productive design methods and form certain recommendations on their application for different tasks and applications is relevant.

Analysis of recent research and publications

Fast and widespread distribution of NoSQL (DB) databases is due to the ease of working with them. NoSQL DB is convenient to use for many modern applications that aim to use scalable databases with high performance, wide functionality, ability to provide maximum usability [4, 6]. For such as mobile, gaming, Internet applications, etc.

Document-oriented DBs are quite common among NoSQL systems. They allow developers to store and query data in the DB using the same document model they used in the program code. Each stored record looks like a separate document with its own set of fields. Documents are flexible and hierarchical, allowing them to evolve to meet the increasing needs of applications. MongoDB, CouchDB, and Couchbase are all examples of the most common document DBMSs. They aim to provide functional and intuitive APIs for agile development. Among them, MongoDB is not only one of the most popular (or widespread), but also very attractive for developers due to the availability of drivers for different programming languages [1 - 2].

Another rather popular type of NoSQL DB is graph DB [3]. Graph DBs implement data representation in the form of nodes and edges, which are relations between

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2524-2296 (online)*

nodes. Such DBs implement easy processing of complex related data and computation of specific properties of graphs, such as the path from one node to another and its length. Common examples of the use of graph DBs include social networks and services; Neo4j is currently the most common on this class of DBMS, since it supports a purely graph model and is already a proven development for production solutions.

DB theory and practice have long established a stage-by-stage approach to their design through conceptual, infological (or ER-) modeling to logical and then physical modeling [7 - 9]. For relational DBs, all transitions from one model to another all transitions from one model to another have been long formalized and unified. However, unfortunately, for NoSQL systems such unified methods of logical design, where it is necessary to take into account the peculiarities of the logic of such systems, do not exist today. For example, usually NoSQL DBs do not involve relational links, so the implementation of similar logic and data integrity mechanism is entirely up to the developers of the corresponding DB.

The current recommendations and approaches do not give developers for NoSQL systems any knowledge about how to model entities and relationships effectively for a particular data model, which data indexes work best, and so on [2, 6, 8]. For example, MongoDB recommends using the "Manual reference" method to create similar logic to links [10 - 11]. [10 - 11], which involves saving the "_id" field of one document to the field of another object, similar to the foreign key in relational DBs, but without supporting the link itself. This method forms a 0:M relation, which can be used by developers as 1:1, 1:M relations and derivatives thereof. But this leads to the "N+1" problem, as it requires an additional query or join data through a JOIN-like operation. Accordingly, document DBs need to use composition in the form of nested objects or arrays of objects to solve such problems. This approach is suitable if the relationship between objects can be expressed by the word "includes".

This approach can be used to model relationships:

- 1:1 type, but it should be considered that embedded object would increase the weight of the document, which slows down its unloading from DB to the client.

- 1:M type, but if M is not a particularly large number and embedded objects should not be too large.

Keep in mind that MongoDB has a maximum nesting size of 100 levels; the maximum document size is 16 MB. Consequently, if new records are constantly being added to the document field (array), the document size will keep growing. This can cause performance problems by moving the document to a different memory location, because there is no place for it to grow in the current location, so defragmentation is performed.

No joins means no JOINs in the relational sense. However, later, MongoDB added two ways of combining data:

- $lookup – an operation that works analogous to LEFT OUTER JOIN in relational DB (added in version 3.2);

- $graphLookup – creates a collection of records showing a hierarchy of objects from some to the current one, similar to lookup in graph DBs (added in version 3.4).

This approach can be used to model relationships:

- 1:1 type, but you have to consider that an embedded object will increase the weight of the document, which slows down its unloading from DB to the client.

- 1:M type, but if M is not a particularly large number and embedded objects should not be too large.

Things are more complicated with entities that have an M:M relation. It is known that an M:M relation can be defined as two 1:M relations and an intermediate object containing identifiers of those two referenced entities [12]. This approach can be implemented in MongoDB without much trouble, except for creating field indexes with identifiers. With this approach, all the auxiliary attributes of the M:M link will be located in a separate object.

But if a developer needs to connect such a link data, he would have to use two JOIN-like operations ($lookup), which in the context of document DB is very expensive.

To solve such a problem, MongoDB practically always uses another approach: compositing this intermediate object into one of the M:M link objects in the form of an array. Figure 1 shows both approaches: via auxiliary entity (top) and reduced composition approach (bottom).

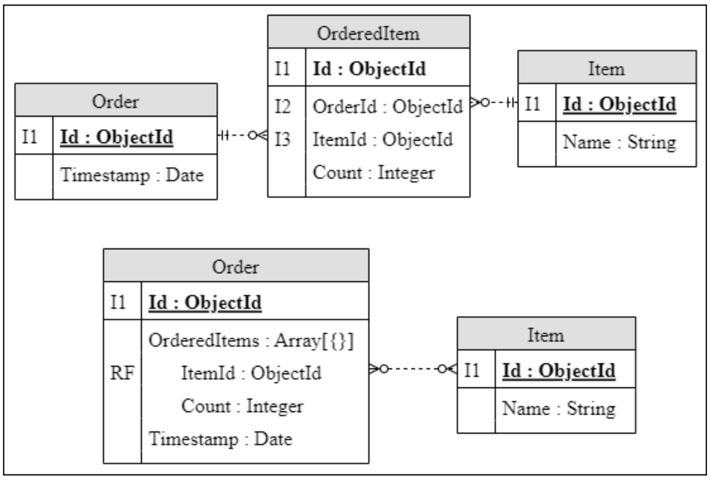


Fig. 1. Approaches to designing M:M communication in document DBs

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

The widespread use of the second approach is due to the fact that in 2017 the $lookup operation gained support for using arrays of identifiers as inputs to connect data. This approach requires only one JOIN operation instead of two to connect the data. But, when using it, you need to clearly identify the "main" M:M connection object, which will contain the identifier array.

Unlike document databases, graph databases support links, although they are quite different from relational links [13]. In Neo4j, each relationship is an entity of a special type that preserves a reference to the outgoing and incoming entities. Thus, links have names, can contain attributes, and indexes can be created on them. Like all NoSQL databases, this DBMS has no integrity restriction mechanisms; this must be decided by the developer at the application level only. But, each relationship in the graph must have a source and an input entity.

It follows that every Neo4j relationship has a default cardinality of 1:M, which can be "transformed" into a 1:1 relationship due to uniqueness constraints or at the software level. Thus, an M:M relationship can potentially be modeled in two ways: through an auxiliary entity (as in relational DBs) and directly by storing additional data as attributes of the relationship. Figure 2 illustrates these modeling approaches graphically: as it looks in relational DB (top), auxiliary entity (middle), and via link attributes (bottom).

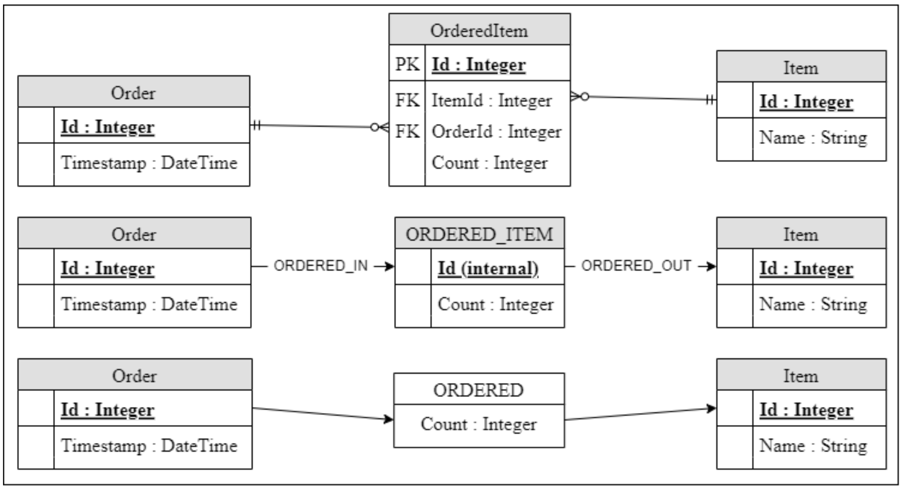


Fig. 2. Comparison of M:M communication design methods in graph DBMS

It should be noted that almost all graph DBMSs have only unidirectional links. The standardized query language Gremlin, supported by all graph DBMSs, also has no support for bidirectional links. Thus, to model bidirectional links, you need to make two bindings in both directions. But considering that a link is also one of the DBMS objects, the option with the intermediate entity is ineffective from the very beginning, as it strongly clogs the DB with redundant entities and links, increases the weight of the DB due to redundant objects and potentially increases the execution time even for basic queries.

However, the existence of the considered recommendations and approaches does not provide NoSQL DB developers with unified methods of logical design of such DB, which would unambiguously indicate the effectiveness of the model obtained in the end. Thus, the study of NoSQL database logical modeling methods and approaches is relevant.

The **aim** of this article is the development of unified logical design methods for NoSQL systems MongoDB and Neo4j based on the analysis of existing design approaches, as well as experimental study of their performance.

This research requires:

- development of unified logical design methods for selected NoSQL databases MongoDB and Neo4j;
- analysis and infological modelling of a certain applied subject area of creation of complex server systems for further experimental research;
- developing of the logical models for the selected DBMS on the basis of the developed unified logical design methods;
- experimental study of the performance of the obtained models and development of recommendations on the feasibility of using the proposed methods in the design of NoSQL databases.

Evaluation of the effectiveness of the methods should be made taking into account such criteria as: disk space occupied by DB (MB); query execution time (ms); operating memory consumption (MB); CPU time consumption (%).

Materials and methods

For further study, the applied subject domain of an arbitrary game server system was chosen. A multiplayer action-adventure game with RPG elements and a dedicated server was chosen as the subject domain object. In games of similar genre and implementation of multiplayer, in any case, it is necessary to implement DB for storing world state and player progress. Consequently, the database must store the following information:

- player account information (currency, player data);
- status and information about the characters in the game world and their abilities;
- a list of the character's tasks and their status;

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

- a list of enemies (monsters) in the game and related information (or information about their location, if the server part generates them);
- a list of non-player characters (NPCs) and related information;
- history of events in the game (buying in-game currency, defeating enemies, completing tasks, etc.).

A general diagram of the domain classes, describing the essence of the game system and the relationship between them, is given in figure 3.

Based on this diagram, as well as the identified integrity constraints and attributes of the subject area, an ER diagram [12] of DB (fig. 4) based on the "Crow's foot" notation was developed. [9].

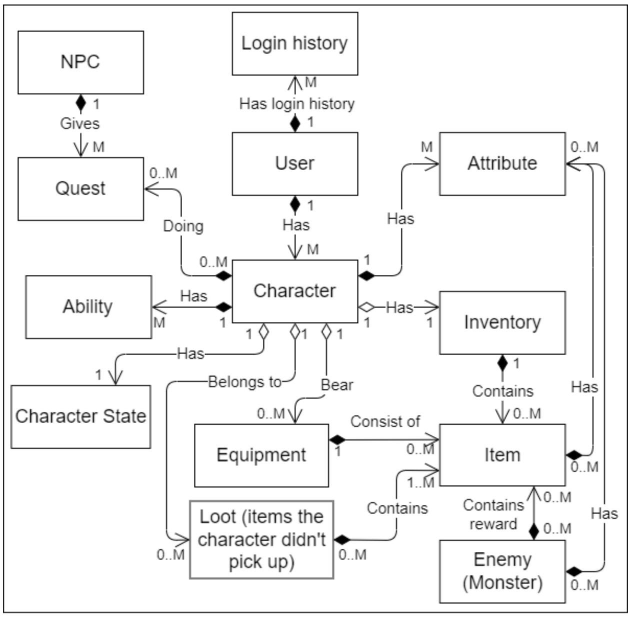


Fig. 3. General class diagram of the subject area

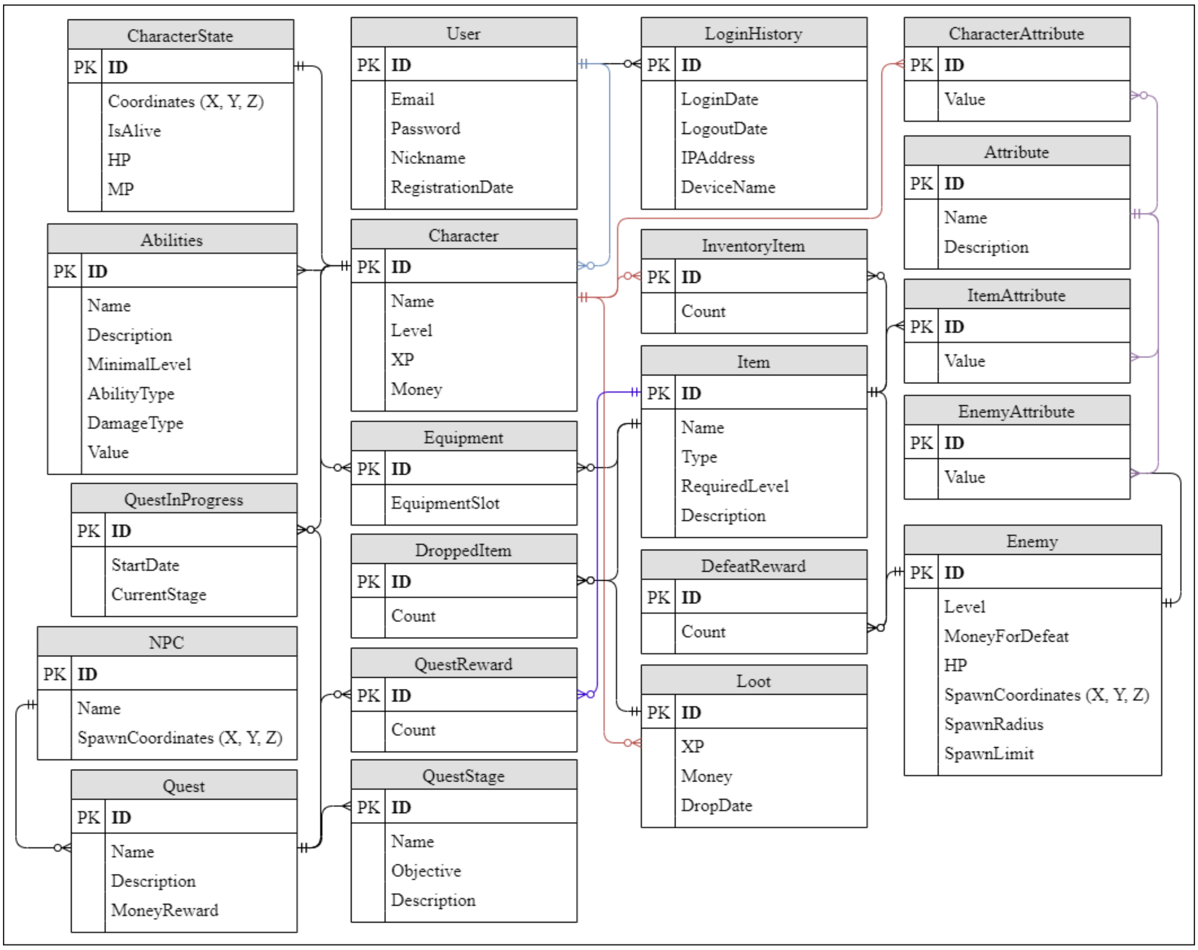


Fig. 4. ER-diagram of the subject area database

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

So, let us consider the methods by which the logical DB design for DBMS MongoDB can be performed. Recall that there is no standardized notation for the visualization of this model. What also complicates the process is that MongoDB objects can have up to 100 levels of nesting and is problematic to reflect visually, although this does not happen very often in practice. Therefore, a modification of the notation for relational logical models with additional functionality inherent in document DB is proposed to describe the document logical model.

Consequently, the mentioned "Manual reference" approach essentially makes the model more similar to relational DBs, so it can be denoted as a "normalizing" method. In contrast, the nested document approach reduces the level of normalization through composition, so it can be called "denormalizing".

Let us consider a unified method for turning an ER diagram into a normalized document logical model, in which the following steps have been proposed:

- modeling entities participating in a 1:1 relationship: add a field with the identifier of one document (master) to another document (dependent).

- modeling entities participating in a 1:M relationship: add a field with the identifier of the main document (1) to the dependent ones (M);

- modeling entities participating in the M:M relationship should use one of the previously mentioned approaches: either through isolating an intermediate entity with identifiers of objects referring to it (more often inefficient), or through composing this intermediate entity. Entity in the "main" object as an array (usually efficient).

The normalized logic model designed by this method is shown in figure 5. All "conditional" external keys constructed by "manual reference" are marked with RF in the figure. The resulting links have purely conditional character due to the fact that MongoDB has no integrity restriction mechanisms and document binding functionality in general. The task of data integrity control is entirely up to the developer.

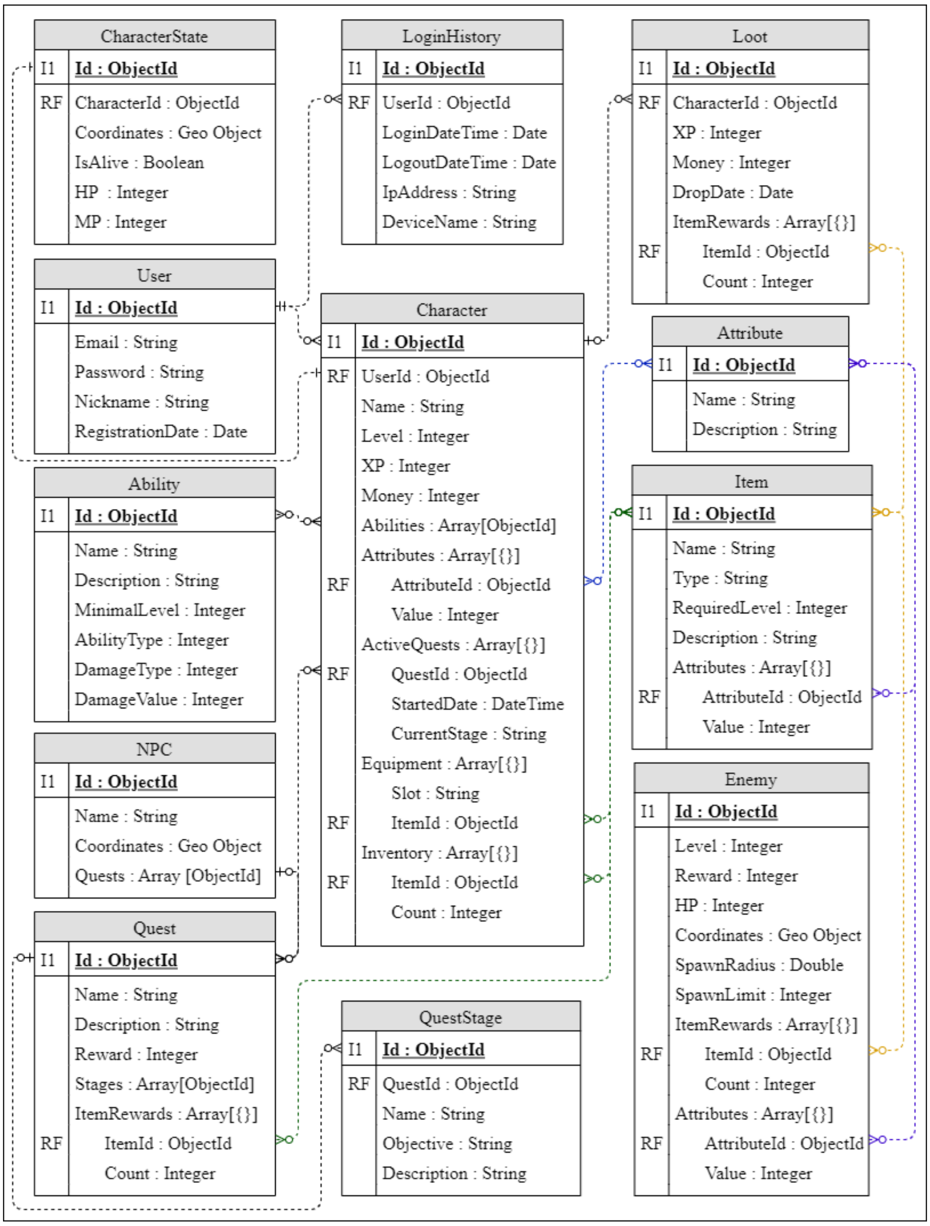


Fig. 5. Normalized DB document logical model of the subject area

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

Consider a unified method for transforming an ER diagram into a denormalized document logical model (fig. 6), in which the following steps have been proposed:

- modeling entities participating in 1:1 relationships: create a field in the main document and nest the dependent document in it, followed by deleting the dependent entity; it is recommended to add an index to it if you plan to select these entities separately from the main entity;

- modeling entities participating in 1:M relationships: add a field-array to the main document (1) containing all dependent (M) entities. If semantically the main entity may have no relations to all dependent entities (no "owns" relation), a separate collection without relations must be created to contain all instances of dependent entities. Otherwise, an additional entity is not required.

- modeling entities that participate in M:M relationships: to add a field-array to the main document that contains all dependent documents. The cases in which an additional collection needs to be created are similar to 1:M.

Guided by this method, a denormalized document logical model of the domain was designed (fig. 6).

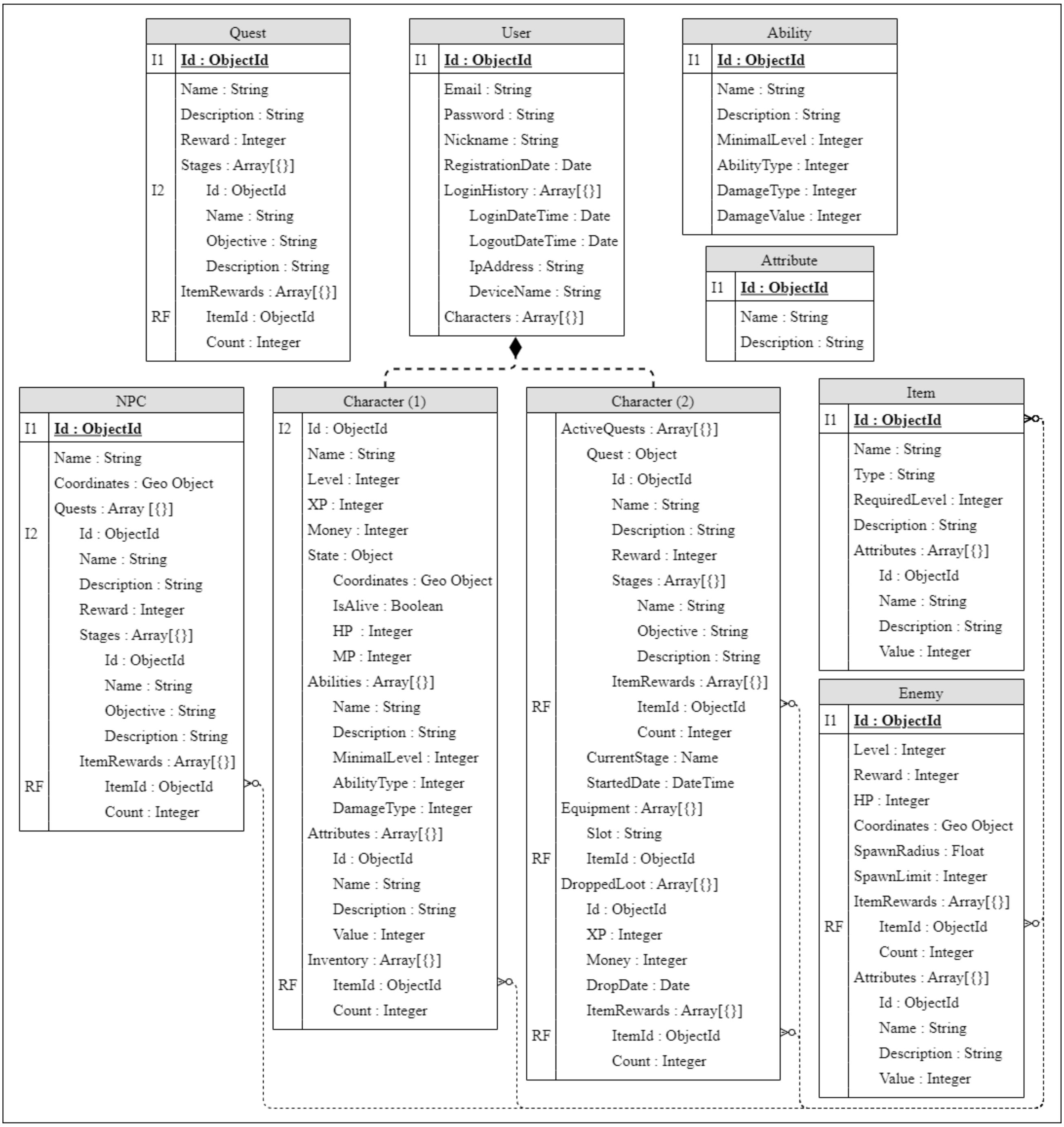


Fig. 6. Denormalized DB document logical model of the subject area

For a more convenient visual representation of the model, the nested Character object has been separated and split into two parts. To denote the nesting of Character in User, the connection with UML class diagrams "including" was used. The only entity that did not undergo denormalization was Item. This is due to the fact that in

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

game applications of this genre all items are accessed by its identifier and the set of all items is unloaded at the start of the game. Thus, JOIN-like operations with the Item entity will not be performed in practice and there will be no difference in performance either.

Next, let's propose a logical design method for the graph model. There is no standardized notation for constructing a logical model of this type now either, so a relational modification will be used. It should be noted that Neo4j supports attributes in relationships, which can significantly reduce the number of entities and simplify the model.

The algorithm for turning an ER diagram into a graphical logic model is very different from the previous ones because of the different structure of data storage. The following steps are proposed for it:

- to combine entities that have 1:1 relationships with each other into one entity;
- to turn 1:M links into graph links without attributes.
- to replace intermediate entities that create M:M links with graph links (with attributes, if any).

Figure 7 shows the graphical logic model obtained as a result of the proposed method.

In the developed model there are two types of links: with and without attributes. A separate notation in the form of a transparent block was proposed to display links with attributes. The use of attribute relationships eliminated all the entities that were used to model the M:M relationship, which reduced the model considerably. But since graph DB does not support nesting of entities, the 1:1 link must be maintained at the program level [13], such as the link between a character and its state.

Thus, as a result of the analysis and modeling of the subject area, logical models were developed: normalized and denormalized document and graph models. Based on these models, the corresponding physical DB models for the corresponding DBMS MongoDB and Neo4j were developed for further study.

For the experimental study the clusters from DB servers or source-replica type replication were used, as this approach is suitable for game servers with large read specificity. Consequently, all measurements were performed on clusters of database servers regardless of configuration. They were located in the Azure cloud service on virtual machines of different sizes.

Thus, the following DB server configurations with their characteristics were chosen for the experiments:

- configuration type Small: machine name – Standard_B2s; vCPU - 2; RAM - 4 GB; number of nodes - 2; number of connections 20;
- configuration type Medium: machine name is Standard_B4ms; vCPU - 4; RAM - 16 GB; number of nodes - 4; number of connections 50;
- configuration type Large: machine name – Standard_B8ms; vCPU - 8; RAM - 32 GB; number of nodes - 6; number of connections 100.

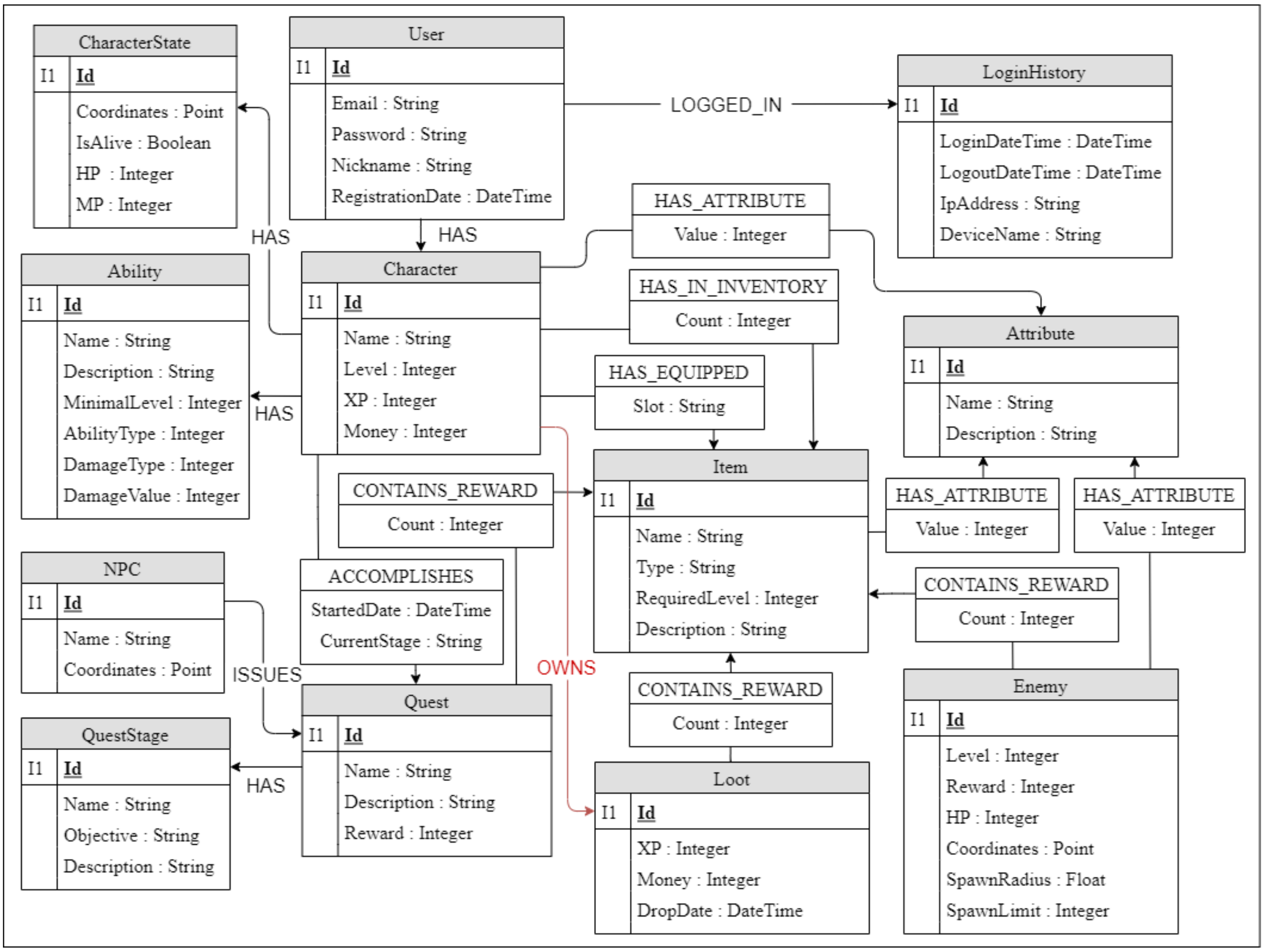


Fig. 7. Graphical logic model of the subject area database

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

Ubuntu 20.04 LTS Minimal was used as the operating system to minimize the consumption of resources by the system. The type of machine configuration also affects the number of entities in the DB to be used in the experiments (table 1).

Table 1. *Number of DB entities for experiments on configurations*

Type of configuration	Small	Medium	Large
Users / characters per user	3000 / 1	5000 / 2	8000 / 3
Number of entries in the game per user	25	50	75
Total items in inventory of the players	100 / 50	200 / 100	300 / 150
Skill / equipment slots	10 / 4	25 / 6	50 / 8
NPCs/tasks they issue	50 / 100	150 / 200	300 / 500
Enemies	100	200	500
Loot / number of items within it	5000 / 3	15000 / 5	30000 / 8
Number of DB items in the "worst case" (denormalization)	776 967	4 701 983	16 362 659

Based on games of a similar genre, it was taken into account that some entities cannot be in large numbers and do not change depending on the configuration, for example: Attribute (a constant number - 6 was chosen); CharacterState (one entity per character).

When performing each step of the experimental study, it was decided to collect metrics that are quite often used to investigate DB performance [14 - 15]:

- S – space occupied by DB on disk (MB);
- M – RAM consumption (MB);
- C – processor time consumption (%);
- T – query execution time (ms) (the results of experiments to measure this metric will be given in the further publications);

Results of research and their discussion

Let us consider the main most interesting performance trends of the experiments to study the designed models for NoSQL DBMS MongoDB and Neo4j.

First of all, let's compare DB sizes with filled test data, which is shown in figure 8.

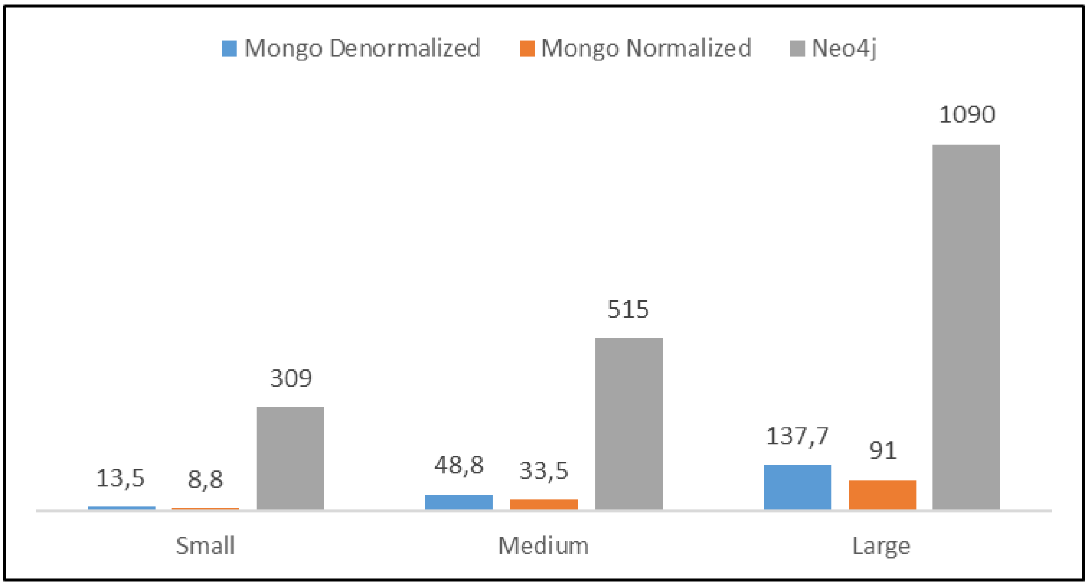


Fig. 8. DB size comparison (on disk)

The diagram shows that DBMS Neo4j consumes a huge amount of disk space, and this growth is almost linear to the number of entities. In the course of experiments it was determined that this "DB weight" is formed by entities, the connections themselves practically do not take up disk space. The denormalized MongoDB model weighs 30-35% more than the normalized one, which is obviously caused by data redundancy. Nevertheless, in terms of DB weight MongoDB clearly wins over Neo4j.

The results of the comparison of RAM consumption of the DBMS server are shown in figure 9.

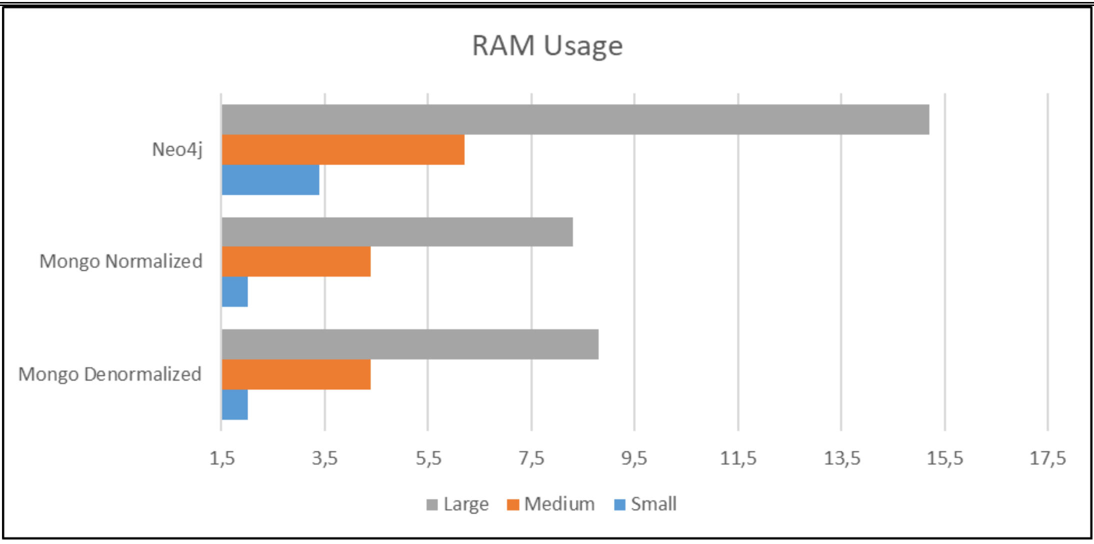


Fig. 9. RAM usage

The histogram shows that Neo4j uses even more RAM than MongoDB. In this situation, the MongoDB memory allocation logic still plays a role: DBMS cannot use more than 50% of the system RAM, while Neo4j, if necessary, can use almost all available to it. Also, Neo4j has conditionally minimal amount of RAM for the correct work - 2 gigabytes, when the recommended amount is about 8 gigabytes.

Let's consider the results of measurements of CPU usage by the DBMS server. Three configurations were used in the research. So, the experiments have shown that for small projects or projects at MVP stage Neo4j is not especially effective. Let's take a closer look at the Medium configuration (fig. 10), which more corresponds to the real machines configurations for medium-sized projects.

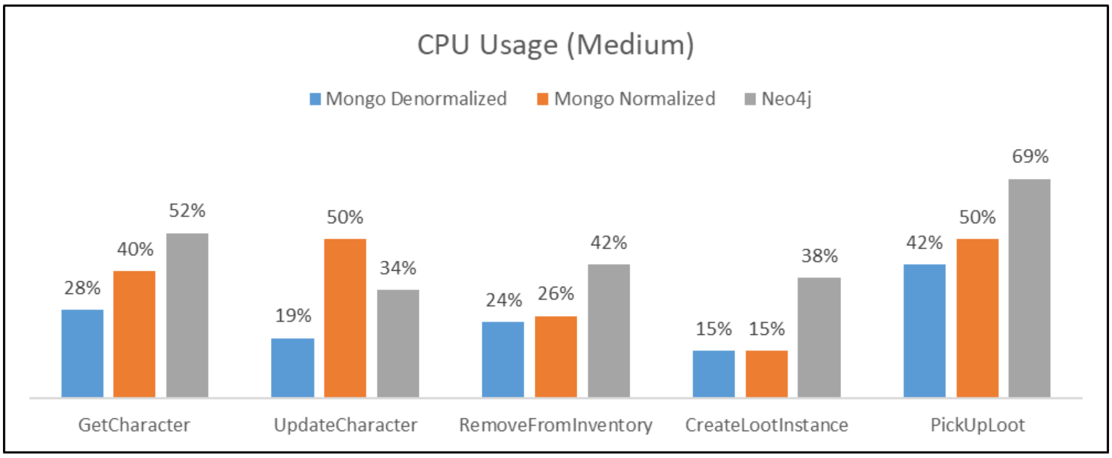


Fig. 10. CPU usage (Medium configuration)

With so many resources, the situation for Neo4j has leveled off relative to MongoDB, now the DBMS data is about equal. In general, it was on this configuration that Neo4j started working "without limitations". We can even conclude that the resources allocated to it are even a bit much for the load that was allocated to it.

Figure 11 shows the results of the measurements for the Large configuration. In general, the situation is very similar to the preliminary results. The resources increased, but the DB size and load increased proportionally to the resources.

We see that the allocated DBMS resources are more than they need for stable operation on these loads.

We also investigated the performance of the models when executing queries. But this will be a topic for another publication. Note only that during all comparisons we could see certain pattern - Neo4j consumes more resources compared to MongoDB, denormalized model works faster than normalized model in context of the queries studied as well as requires less resources.

After all experiments, we can unequivocally say that the denormalized MongoDB model is the most preferable option for the studied domain (DB model and queries). This scheme resulted in the lowest consumption of machine resources with satisfactory performance.

After comparing all the results obtained, we can draw some conclusions and develop some recommendations for the use of one or another method in a particular situation.

So DBMS Neo4j. It has been in development for 15 years, during which it has acquired a large set of functionalities, significant performance improvements and so on. But in practice, it is not so good: the limitation of Community version, huge consumption of CPU and RAM

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

resources, large DBMS weight compared to other DBMS and average performance in trivial tasks make this DBMS not particularly attractive for small or medium sized projects. It is also should be noted that the demanding DBMS is also associated with its implementation of JVM, which immediately impose restrictions on the smallest RAM for the DBMS server.

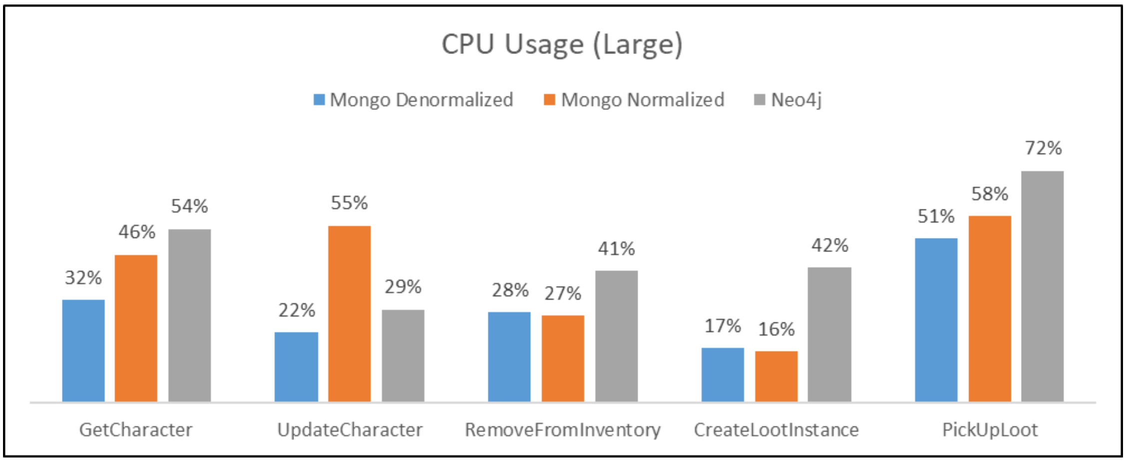


Fig. 11. CPU usage (Large configuration)

One of the peculiarities of Neo4j is that it uses the maximum of its allocated resources, so they have to be strictly limited to certain values. But it should be noted that this DBMS is able to easily perform operations that are difficult or impossible to perform in other DBMS.

Thus, it is recommended to use graph model logic design method and use Neo4j in cases when:

- ER graph DB contains a large number of M:M links and the server-side logic involves frequent fetching of several linked data simultaneously;
- an ER diagram DB has a small fraction of entities on a large fraction of links, and the application logic is mostly about deleting and adding links between DB objects;
- the system is large, has a large number of users and the company has a large amount of resources;
- the server side needs the specifications of graph DB, such as finding the depth of relationships.

Now let's move on to DBMS MongoDB. Consider first the model normalization method. Using this method resulted in zero data redundancy in the DB, which had a positive effect on weight. Also, since the DB objects are much smaller than the denormalized model, they have more "similarity" between them, DBMS more effectively applied the compression mechanism of the stored data (on average, by 5-15%).

But the analyzed operations in the server system under study often required either joining data or performing operations on several collections simultaneously, which required the use of transactions or JOIN-like operations. This resulted in reduced performance compared to the denormalized model.

Thus, the normalization method should be used if:

- the links in the schema are predominantly cardinality "0", which eliminates the need to artificially maintain data integrity through transactions (the traditional "eventually consistent" approach);
- in a 1:M relation, the number M is expected to be large (and/or the weight of the object is large). This is due to an object size limit of 16 MB;
- the system was previously using a relational RDBMS and a quick migration to MongoDB is required.

The denormalization method used in the server system under study proved to be the most efficient in terms of performance. Also data redundancy increased the weight of DB noticeably. Also some operations of the system were quite difficult to implement using array operations (and some potentially impossible), which is not typical for normalized model. This method should be used if the number of "M" objects in a 1:M relationship is not particularly large (up to 1000) or dependent objects cannot exist without the main one (simpler "artificial" data integrity support);

Conclusions and prospects for further development

In this study, NoSQL DB logical design methods were proposed and investigated in terms of performance using DBMS MongoDB and Neo4j examples. A series of experiments were conducted to measure the resources consumed.

Based on the analysis of logical design approaches, unified logical design methods for NoSQL systems MongoDB and Neo4j were proposed. For the experiment, based on the proposed methods, logical models were designed, the performance of which was investigated. The experiments used metrics on the resources required to handle such models.

The study showed that none of the proposed modeling methods for MongoDB could be called unambiguously best. The best would be a mixed method - a combination of modeling through normalization and denormalization. In general, it can be unambiguously said that both studied DBMS have good performance, although they are oriented to different tasks.

If you don't know in advance how fast the system will grow, how many users it will have, and so on, a universal choice is to use MongoDB. This DBMS has a very wide functionality and the ability to scale

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

horizontally and vertically, which makes it a good choice for prototypes and newly created systems.

Thus, based on the results of the experimental study, recommendations for the use of the proposed methods have been formed. These recommendations can be used to design real systems, in particular in the area of game servers.

References

1. Maran, M. M., Paniavin, N. A., Poliushkin, I. A., (2020), "Alternative Approaches to Data Storing and Processing", *V International Conference on Information Technologies in Engineering Education (Inforino)*, P. 1–4, **DOI**: https://doi.org/10.1109/inforino48376.2020.9111708
2. Meier, A., Kaufmann, M. (2019), *SQL & NoSQL Databases: Models, Languages, Consistency Options and Architectures for Big Data Management*, Springer Vieweg, , 248 p. **DOI**: https://doi.org/10.1007/978-3-658-24549-8
3. Wood, P. T. (2018), "Graph Database", In: Liu, L., Özsu, M.T. (eds), *Encyclopedia of Database Systems. Springer*, New York, NY, P. 1639–1643. **DOI**: https://doi.org/10.1007/978-1-4614-8265-9_183
4. Acharya, B., Jena, A. K., Chatterjee, J. M., Kumar, R., & Le, D. (2019), "NoSQL Database Classification: New Era of Databases for Big Data", *International Journal of Knowledge-Based Organizations (IJKBO)*, 9 (1), P. 50–65. **DOI**: http://doi.org/10.4018/IJKBO.2019010105
5. Halpin, T., Morgan, T, (2008), "Information Modeling and Relational Databases (Second Edition) ", *The Morgan Kaufmann Series in Data Management Systems*, P. 305–343. **DOI:** https://doi.org/10.1016/B978-0-12-373568-3.X5001-2
6. Kuzochkina, A., Shirokopetleva, M., Dudar, Z. (2018), "Analyzing and Comparison of NoSQL DBMS", *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, P. 560–564. **DOI**: https://doi.org/10.1109/INFOCOMMST.2018.8632133
7. Sanders, G. L., Shin, S. K. (2001), "Denormalization effects on performance of RDBMS", *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, P. 9–15.
8. Sahatqija, K., Ajdari, J., Zenuni, X., Raufi, B., Ismaili, F., (2018), "Comparison between relational and NOSQL databases", *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, P. 216–221. **DOI**: https://doi.org/10.23919/mipro.2018.8400041
9. Date, C. J. (2019), *Database Design and Relational Theory: Normal Forms and All That Jazz*, Apress, 470 p, ISBN 978-148-425-539-1. **DOI**: https://doi.org/10.1007/978-1-4842-5540-7
10. Palanisamy, S., SuvithaVani, P. (2020), "A survey on RDBMS and NoSQL Databases MySQL vs MongoDB", *International Conference on Computer Communication and Informatics (ICCCI)*. **DOI**: https://doi.org/10.1109/iccci48352.2020.9104047
11. Chodorow, K., (2016), *MongoDB: The Definitive Guide: Powerful and Scalable Data Storage, 3rd Edition*, O'Reilly Media, 514p.
12. Bagui, S., Earp, R. (2011), *Database Design Using Entity-Relationship Diagrams (Foundations of Database Design)*, Auerbach Publications, 371 p. **DOI:** https://doi.org/10.1201/9781439861776
13. Vukotic, A., Watt, N., Abedrabbo, T., Fox, D., Partner, J. (2014), *Neo4j in Action*, Manning, 304 p.
14. Mazurova, O., Naboka, A., Shirokopetleva, M. (2021), "Research of ACID transaction implementation methods for distributed databases using replication technology", *Innovative technologies and scientific solutions for industries*, № 2 (16), P. 19– 31. **DOI**: https://doi.org/10.30837/ITSSI.2021.16.019
15. Gomes, C., Borba, E., Tavares, E., Junior, M. N. de O. Performability (2019), "Model for Assessing NoSQL DBMS Consistency", *IEEE International Systems Conference (SysCon)*. **DOI**: https://doi.org/10.1109/syscon.2019.8836757

Received 30.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Мазурова Оксана Олексіївна – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри програмної інженерії, м. Харків, Україна; email: oksana.mazurova@nure.ua; ORCID ID: https://orcid.org/0000-0003-3715-3476.

Мазурова Оксана Алексеевна – кандидат технических наук, доцент, Харковский национальный университет радиоэлектроники, доцент кафедры программной инженерии, г. Харьков, Украина.

Mazurova Oksana – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Radio Electronics, Associate Professor of the Department of Software Engineering, Kharkiv, Ukraine.

Сиволовський Ілля Михайлович – магістр, Харківський національний університет радіоелектроніки, м. Харків, Україна; email illia.syvolovskyi@nure.ua; ORCID ID: https://orcid.org/0000-0002-4592-0965.

Сиволовский Илья Михайлович – магистр, Харьковский национальный университет радиоэлектроники, г. Харьков, Украина.

Syvolovskyi Illia – Master, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

Сиволовська Олена Вікторівна – кандидат економічних наук, доцент, Український державний університет залізничного транспорту, доцент кафедри маркетингу, м. Харків, Україна, email: alenasvl3@gmail.com; ORCID ID https://orcid.org/0000-0002-9317-9307.

Сиволовская Елена Викторовна – кандидат экономических наук, доцент, Украинский государственный университет железнодорожного транспорта, доцент кафедры маркетинга, г. Харьков, Украина.

Syvolovska Olena – PhD (Economics Sciences), Associate Professor, Ukrainian State University of Railway Transport, Associate Professor of the Department of Marketing, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2524-2296 (online)*

МЕТОДИ ЛОГІЧНОГО ПРОЕКТУВАННЯ NOSQL БАЗ ДАНИХ ДЛЯ MONGODB ТА NEO4J

Сучасні розробники ігрових мобільних та інтернет-додатків майже не уявляють себе без використання NoSQL баз даних, якщо вони мають на меті створення масштабованих баз даних, які мають високу продуктивність та широкі функціональні можливості. При проєктуванні бази даних для будь-якої NoSQL-системи від розробника вимагається чітке розуміння логіки таких баз даних та можливостей інструментів, які пропонує відповідна СКБД. Але, на жаль, уніфікованих методів логічного проектування таких моделей, як є в реляційних базах даних, вони не мають. Отже існує проблема розробки ефективних методів логічного проектування NoSQL баз даних, які б забезпечували необхідну продуктивність під час реалізації бізнес-логіки відповідних додатків. **Предметом** дослідження є підходи до логічного проектування NoSQL документних та графових баз даних. **Мета** роботи – запропонувати уніфіковані методи логічного моделювання для NoSQL систем MongoDB та Neo4j на основі експериментального дослідження їх продуктивності. В роботі вирішуються наступні **завдання:** аналіз актуальних підходів до логічного проектування документних та графових баз даних, розробка методів логічного проектування для них; планування та експериментальне дослідження продуктивності запропонованих методів на прикладі моделей, що розроблено за їх допомогою. Використовуються такі **методи:** методи проектування та оцінки продуктивності баз даних, методи розробки базуються на СКБД MongoDB 5.0.5, Neo4j 4.4.3, середовищі розробки Visual Studio 2022. Отримано наступні результати: запропоновано уніфіковані методи логічного проектування для NoSQL систем MongoDB та Neo4j; на їх основі розроблено відповідні логічні моделі; проведено експериментальні заміри кількості **Висновки:**ресурсів, що необхідні для роботи з розробленими моделями; сформовано рекомендації щодо запропонованих методів. запропоновані методи моделювання для MongoDB мають власні аспекти ефективного використання для різних типів додатків; були виявлені сильні та слабкі сторони обох методів, але рекомендовано змішаний метод на базі комбінації моделювання через нормалізацію та денормалізацію; незважаючи на те, що Neo4j в більшості експериментів програла MongoDB за споживаними ресурсами, але обидві СКБД мають хорошу продуктивність орієнтовно до різних завдань.

Ключові слова: база даних; метод логічного проектування; СКБД; Neo4j; NoSQL; MongoDB.

МЕТОДЫ ЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ NOSQL БАЗ ДАННЫХ ДЛЯ MONGODB И NEO4J

Современные разработчики игровых мобильных и интернет-приложений почти не представляют себя без использования NoSQL баз данных, если они преследуют цель создания масштабируемых баз данных, имеющих высокую производительность и широкие функциональные возможности. При проектировании базы данных для любой NoSQL-системы от разработчика требуется четкое понимание логики таких баз данных и возможностей инструментов, предлагаемых соответствующей СУБД. Но, к сожалению, унифицированных методов логического проектирования таких моделей, как в реляционных базах данных, они не имеют. Таким образом, существует проблема разработки эффективных методов логического проектирования таких баз данных, которые обеспечивали бы необходимую производительность при реализации бизнес-логики соответствующих приложений. **Предметом** исследования являются подходы к логическому проектированию NoSQL документных и графовых баз данных. **Цель** работы – предложить унифицированные методы логического моделирования для NoSQL систем MongoDB и Neo4j на основе экспериментального исследования их производительности. В работе решаются следующие **задачи:** анализ актуальных подходов к логическому проектированию документных и графовых баз даных, разработка методов логического проектирования для них; планирование и экспериментальное исследование производительности предложенных методов на примере моделей, разработанных с их помощью. Используются следующие **методы:** методы проектирования и оценки производительности баз данных, методы разработки базируются на СУБД MongoDB 5.0.5, Neo4j 4.4.3, среде разработки Visual Studio 2022. Получены следующие **результаты:** предложены унифицированные методы логического проектирования для NoSQL систем MongoDB и Neo4j; на их основе разработаны соответствующие логические модели; проведены экспериментальные замеры количества ресурсов, необходимых для работы с разработанными моделями; сформированы рекомендации по предложенным методам. **Выводы:** предложенные методы моделирования для MongoDB имеют собственные аспекты эффективного их использования для разных типов приложений; были выявлены сильные и слабые стороны обоих методов, однако рекомендовано смешанный метод на базе комбинации моделирования через нормализацию и денормализацию; несмотря на то, что Neo4j в большинстве экспериментов проиграла MongoDB по потребляемым ресурсам, обе СУБД демонстрируют хорошую продуктивность с учетом ориентации на разные задания.

Ключевые слова: база данных; метод логического проектирования; СУБД; Neo4j; NoSQL; MongoDB.

Бібліографічні описи / Bibliographic descriptions

Мазурова О. О., Сиволовський І. М., Сиволовська О. В. Методи логічного проектування NoSQL баз даних для MongoDB та Neo4j. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 52–63. DOI: https://doi.org/10.30837/ITSSI.2022.20.052

Mazurova, O., Syvolovskyi, I., Syvolovska, O. (2022), "NoSQL database logic design methods for MongoDB and Neo4j", *Innovative Technologies and Scientific Solutions for Industries,* No. 2 (20), P. 52–63. DOI: https://doi.org/10.30837/ITSSI.2022.20.052

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 004.42 DOI: https://doi.org/10.30837/ITSSI.2022.19.064

M. PERETIATKO, M. SHIROKOPETLEVA, N. LESNA

RESEARCH OF METHODS TO SUPPORT DATA MIGRATION BETWEEN RELATIONAL AND DOCUMENT DATA STORAGE MODELS

The **subject** matter of the article is heterogeneous model-inhomogeneous data migration between relational and document-oriented data storage models, existing strategies and methods to support such migrations, the use of relational algebra and set theory in the context of databases in building a new data migration algorithm. The **goal** of the work is to consider the features and procedure of data migration, explore methods to support data migration between relational and documentary data models, build a mathematical model and algorithm for data migration. The following **methods** were used: analysis and comparison of existing approaches to data migration, choice of strategy for further use in compiling the migration algorithm, mathematical modeling of the algorithm of heterogeneous model-inhomogeneous data migration, formalization of the data migration algorithm. The following **tasks** were solved in the article: consideration of the concept and types of data migration, justification for choosing a document-oriented data model as a target for data migration, analysis of existing literature sources on methods and strategies of heterogeneous model data migration from relational to document-oriented data model, highlighting advantages and disadvantages existing methods, choosing an approach to the formation of the data migration algorithm, compiling and describing a mathematical model of data migration using relational algebra and set theory, presentation of the data migration algorithm, which is based on the focus on data queries. The following **results** were obtained: the possibilities of relational algebra and set theory in the context of data models and queries are used, as well as in model redesign, the strategy of migration of data models is chosen, which provides relational and document-oriented data models, the algorithm of application of this method is described. **Conclusions:** because of the work, the main methods of migration support for different data storage models are analyzed, with the help of relational algebra, set theory a mathematical model is built, and an algorithm for transforming a relational data model into a document-oriented data model is taken into account. The obtained algorithm is suitable for use in real examples, and is the subject of further research and possible improvements, analysis of efficiency in comparison with other methods.

Keywords: database; heterogeneous migration; data model; set theory.

Introduction

Today, the role of information technology is increasing in the world; there is a growing number of software applications covering a variety of areas of people's lives. Most software applications involve the storage of data in one form or another. As the role of software systems grows, the scope of their use expands, the amount of data storage required increases, and the structure of data becomes more complex. Data storage methods are also evolving: new approaches to data storage are developed, new types of databases are created, existing database management systems are improved, hybrid databases that contain properties and functions of several other databases appear, etc.

Eventually the software system may face the problem of failure to function fully due to the limitation of the database used:

- with an excessive load on the database reaching its limits with a large number of system users;
- with increasing complexity of business logic and, as a consequence, difficulty of using the data model of the current database for the needs of this business logic;
- with the transition of a software application to a new technology stack and the technical or logical complexity of using the current database with the new technology stack;
- the impossibility of development and competitiveness of a software system in today's market while using an outdated database in that system (according to Moore's law [1], approximately every two years there is a significant increase in the speed and capabilities of technology, which means that to maintain competitiveness it is always important to be one step ahead of progress);
- when there are risks of full-fledged security and data integrity for outdated DBMSs, etc.

One way to solve the above problem is to migrate to another DBMS (newer, with advantages in features required for a particular software system), with the existing data being migrated to the new database without loss or damage and ready to fully function in the new database this process is called migration.

Database migration is a rather complicated and time-consuming process as the source database and the database to be migrated to may be of different types and have completely different data storage models, data types, ways of working with data, specifics of functioning (for example, migration from relational databases to document-based, event-based, graph-based, etc.).

In order for the migration process to be successful, it is necessary to have a clear migration plan, which includes:

- all preparatory actions for migration;
- conditions and activities in the framework of the migration itself;
- actions after data migration is completed (how the software application will migrate to the new database and how the old database will be liquidated).

Statement of the problem

Within the framework of this work it is necessary to investigate questions of support of migration from relational data model to document-oriented data model, this research should include consideration and analysis of existing methods for this kind of migration and development of own method, as a result of which

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

introduction the newly created data scheme will as much as possible respond to requests to database. Thus, it is necessary to formalize the developed method, i.e. to execute its mathematical modeling and to present in the form of the full-fledged algorithm that in the further researches can be applied on real databases, to carry out the analysis of efficiency at various conditions of use in comparison with other methods.

Literature review

A large number of literary sources are devoted to the issue of database migration. When writing this paper, we used scientific literature, articles from periodicals, publications, as well as web resources that discuss information related to the concepts, principles and methods of data migration.

The concept and fundamental aspects of the theory of database migration are presented in the work of John Morris [2]. A description and comparison of two types of migration - homogeneous and heterogeneous - is presented in a technical web resource [3]. Preston Zhang in his book [4] and Andreas Meyer in his publication [5] describe the principles and process of database migration from a practical viewpoint. Lim Fung Gi et al. in their paper [6] address the issue of the need to redesign the data schema when migrating NOSQL databases with different data models.

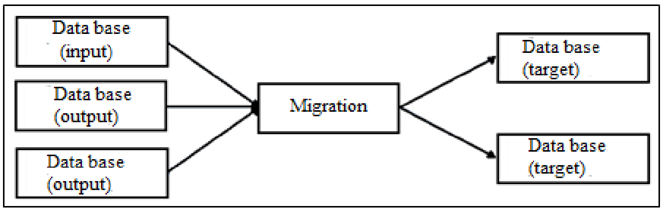
A large number of authors devote their research papers to data migration methods between different data models [7-15]; most of these sources assume not only the physical migration of data between different data stores, but also the data schema re-designing procedure. These methods will be discussed and analyzed in more detail in the following parts.

Analytical review

Database migration is the process of transferring data from one or more source databases to one or more target databases using a specific method [2]. After the migration is completed, the complete, possibly restructured set of source data is contained in the target databases. Customers who used the source databases are migrated to the target databases, and the source databases are not used and can be deleted within a specified period. Figure 1 schematically depicts the database migration process.

In the context of technologies, there are two types of database migration: homogeneous and heterogeneous.

Homogeneous (uniform) migration is a migration between databases in which the source and target databases belong to the same database technology [3], such as migrations from a MySQL database to a MySQL database, or from an Oracle database to an Oracle database. Homogeneous migrations also include migrations between databases systems hosted on its own server, such as PostgreSQL, to its managed version, such as Cloud SQL (a variant of PostgreSQL).



n

Fig. 1. Scheme of the database migration process

For homogeneous migration, the source and target database schemas are identical in most cases. If the schemas are different, the source database data must be converted during migration.

Heterogeneous (uneven) database migration is a migration in which the source and target databases belong to different database technologies [3], for example, migration from MS SQL database to MongoDB. Heterogeneous database migration can be between identical data models (e.g., relational to relational) or between different data models (e.g., relational to key-value). Migration between different database technologies does not necessarily involve different data models. In particular, Oracle, MySQL, PostgreSQL, and Spanner support a relational data model. However, multi-model databases such as Oracle, MySQL, or PostgreSQL support multiple data models. For example, if a multi-model database supports storing data as JSON documents, the data can be ported to MongoDB without the need for a practical conversion because the data model is the same in the source and target databases.

Though the difference between homogeneous and heterogeneous migration is based on database technologies, alternative categorization is based on the database models involved.

For example, migration from an Oracle database to Spanner is model-homogeneous because both databases use a relational data model, that is, only the technology used for the database changes. Figure 2 shows a diagram of heterogeneous model-homogeneous migration.

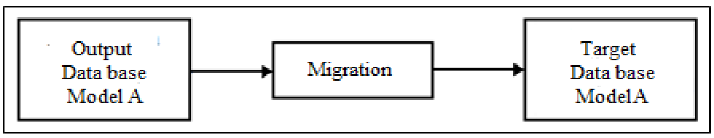


Fig. 2. Heterogeneous model-homogeneous data base migration

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

Migration is model-heterogeneous when different data storage models are used in source and target databases, if, for example, data stored as JSON objects in Oracle are migrated to a relational model in Spanner. Fig. 3 shows a diagram of heterogeneous model-heterogeneous migration.

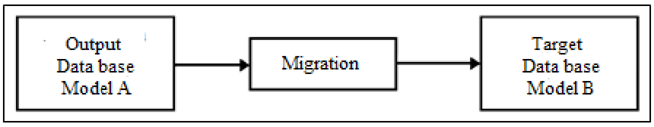


Fig. 3. Heterogeneous model-heterogeneous data base migration

The classification by data model categories more accurately reflects the level of complexity of data migration in comparison with the distribution of database systems.

The most difficult case of migration is the one in which the source and target databases are based on different technologies and at the same time have different data models, it is this case will be further considered and analyzed in the framework of this work.

Upon completion of data movement from the source base to the target base, switch client access to the target base and dispose of the source base.

The process of client switching from source to target databases has several parts [4]:

- to continue the migration clients must temporarily close their connections to the source databases and connect to the new databases;

- having closed client connections to the source databases, the process of transferring the data remaining in the source databases to the target databases. This process is called "draining" and is performed to ensure that all data is migrated to the new databases;

- after the data is migrated, the target databases and client connections should be checked for functionality.

The complete absence of downtime for clients during data migration is not possible, with downtime, there may be cases of inability to process requests, and this jeopardizes the operation of the application, so one of the goals in data migration is to minimize downtime. There are strategies by which downtime can be reduced [5]:

- running test clients in read mode with target databases ahead of time before the migration begins;

- analyzing and adjusting the amount of data to be migrated as migration approaches, partially migrating data in certain portions, the total migration time will increase, but the downtime will decrease;

- connecting new clients to the target databases while the old clients are working with the original databases, as a consequence, reducing the complete migration time to the new databases.

There are several options for the cardinality of database migrations:

- direct mapping (1:1): data from one source database is moved to one target database;

- consolidation (n:1): data from several source databases are moved to a smaller number of target databases, this approach can lead to a simplified database management procedure

- distribution (1:n): data from one source database are moved to a certain (>1) number of target databases. This cardinality can be used, for example, when moving an initial centralized database with regional data to several target regional databases;

- redistribution (n:m): data from a certain number of source databases is moved to a certain number of target databases. Such cardinality is useful in the situation of uneven number of data in the source databases (and, accordingly, uneven load), due to redistribution data are distributed evenly between the target databases.

During data migration, it is possible not only to carry out the actual migration of data, but also to redesign the database [6], more often architectural changes are introduced if the source and target databases have different models, because each type of model includes its own characteristics and principles in which the model will work more effectively, for example, when migrating data from the relational model to non-relational, instead of creating dependent tables, you can move them into nested tables (collections). This will reduce the number of queries to the database and reduce the processing time of related entities.

For this work, it was necessary to choose an example of what kind of NoSQL data model will be further consideration of the material. Considering the information about today's most popular and widely used NoSQL databases [19], it was found that the document-oriented database model MongoDB falls under such criteria. In the overall ranking of databases according to the resource [20], it is in the top 10, being in the fifth position, and ranks first in the NoSQL ranking, since all the previous ones are relational databases. In terms of database popularity, document databases are in second place after relational databases, the percentage of relational databases is 71.9% and document databases is 9.9% [20]. The structure and capabilities of this database have also been analyzed: in particular, there are effective database sharing technologies, formalized models of big data management [21].

A large amount of literature is devoted to comparing MongoDB with relational databases and detailing the advantages of the former [22]. Now MongoDB is used in many subject areas (3D visualization, predicting building thermal capacity usage, groundwater flow control and pollution transport, in health monitoring systems, IoT applications, etc.).

Hence, after the above analysis, it was decided to choose a document-oriented model (using MongoDB as an example) as a NoSQL database for use in the study.

Analysis of existing methods and algorithms

The issue of migration between databases represented by different models is a hot topic at the

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

moment; it has not been studied sufficiently for full formalization, so research related to this issue deserves special attention. There is no unambiguous recommendation for migration in one way or another and the developer himself must make decisions on the method of migration, depending on the characteristics of data and purposes for which migration is carried out.

Let's consider existing approaches and strategies for migrating from a relational database to MongoDB.

One of the more common ways to migrate data from a relational model to MongoDB is based on the fact that most relational databases support exporting tables to CSV format files. Even if there is no such built-in support, it is possible to export using auxiliary software and get the files in the right format. You can then import the files into MongoDB using the built-in command [7]. The disadvantage of this method is that, first, the existing relationships between tables are not taken into account, because essentially only data lists are obtained, and second, each table in the relational database will correspond to a collection in MongoDB, no logical. Architectural rebuilding of tables in document-oriented style, it will affect query execution time, because, as we know, MongoDB works harder with queries that access many document collections. Therefore, this method is reasonable to use only for databases of simple structure with few tables and links.

Another approach to migrating data from relational to MongoDB is migration, which consists of the following sequence of actions [8, 9, 10]:

- extracting data from the original database;
- working with the data, bringing them into the right form (working on data types, etc.)
- transfer of the processed data to the target database.

The disadvantage of this approach is that when working with data, insufficient attention is paid to database schemas and links between objects, because the emphasis is put on the data as such, rather than on their structuring, that is, as in the previous method, when using this strategy there is no restructuring of the data schema.

Another well-known way to migrate data from a relational model to MongoDB is to migrate data based on data structure and data queries [11]. Such migration is performed in three steps:

- describing the relational database structure, describing the data query requirements (according to the business logic);
- modeling the data in the query-oriented context of the NoSql database;
- modeling the database schema in the query-oriented context of the NoSql database.

The disadvantage of this method, as in previous cases, is that it does not take into account the dependencies between database objects, since the new database structure takes into account only metadata about objects and queries.

The next existing approach to this kind of migration is data migration by rules (six rules) describing three types of migration: Column-Based, Document-Based and Graph-Based [12]. The rules describe the cardinality of links between tables and special operations performed on one of the tables (aggregation operations, etc.). The disadvantage of this approach is that the structure of data queries is not taken into account during migration. To solve the problem of query duration that accesses multiple documents, this approach suggests combining all tables into a single NoSQL collection, but this action will inevitably lead to memory problems, because the size of such a collection will be too large. Applying such a method can be justified only if the database was voluminous.

Another method assumes that relationships in a document-oriented model can be represented in the form of embedded documents and relationships between these documents [13, 14]. For example, if there is a functional relationship between two attributes, both attributes will be transformed into a single data element in MongoDB. The same principle is applied for partial and transitive dependencies. The disadvantage is that embedded documents can only be used for a limited amount of data, and there is no clear identification of the form of this embedding.

There is another method, it involves using the theory of database schema normalization and using it in schema design for MongoDB [15], but this approach does not take into account the relationships of "many", primary and foreign keys.

Consequently, after considering the main methods of data migration between relational and json-like data models, we can say that the methods under consideration have their advantages and disadvantages and should be used depending on the specific situation, possibly in combination with each other.

Choice of methods

While studying and analyzing the methods of converting relational data model to MongoDB data model, three main general migration strategies were identified for further consideration and research:

- migration creates a corresponding collection in MongoDB for each relational database table [16];
- during migration, all the relational database tables are merged into a single MongoDB data collection;
- during migration, the database schema is redesigned so that it best meets the database queries (as a consequence, it would simplify the execution of those queries).

The first two strategies are clear and unambiguous and do not require the use of auxiliary methods for implementation.

The third strategy is more complicated and involves the use of auxiliary methods by which the collection schemas in MongoDB would be formed in response to queries.

One of the approaches in transforming data models is the use of relational algebra and set theory [17]. This adapts methods of relational algebra and set theory for convenient use in the context of database models and schemas. Using this approach, it is possible, using a

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

formal language, to develop specific model transformation steps and compose a general algorithm to support heterogeneous model-inhomogeneous migration for selected data models.

The use of relational algebra and set theory is appropriate to implement the strategy of re-designing database schema according to queries, because the hierarchy of model structure and queries is quite convenient to represent by sets (compositions), analyze them, perform actions with these sets and present the results of these actions [18]. Therefore, this approach will be used as a tool for further development of migration maintenance methods.

Mathematical modeling of migration

Let us represent the incoming relational database schema using set theory. Let *T* be the set of all tables in the relational schema, the set *T* consists of elements T_i, where r is the number of table in the schema, in the form of a formula for representing the set of tables looks as follows:

$$T = \{T_i, i = 1,...n\}, \tag{1}$$

where T_i – *i*-th table in the table set *T*;

i – table number in a set of tables;

n – the total number of tables in the scheme. can be combined with one another.

Schematically, a set of tables is shown in fig. 4.

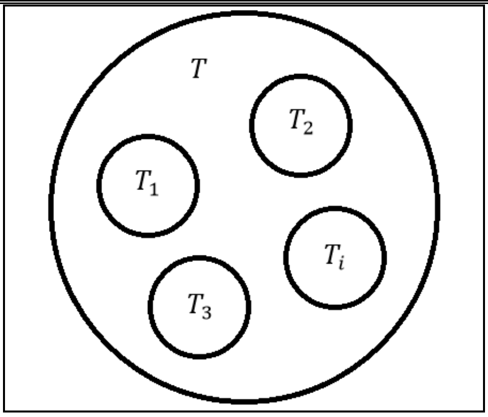


Fig. 4. Representing a relational database schema as a set.

Each table consists of the fields, that is, the table is a set of fields:

$$T_i = \{F_{ij}, i = 1,...n; j = 1,...i_k\}, \tag{2}$$

where F_{ij} – *j*-th field at the *i*-th table;

i – table number in a set of tables;

n – total number of tables in the scheme;

j – field number at the *i*-th table;

i_k – total number of fields in the *i*-th table. can be combined with one another.

The representation of the relational database schema in the form of sets is shown in fig. 5.

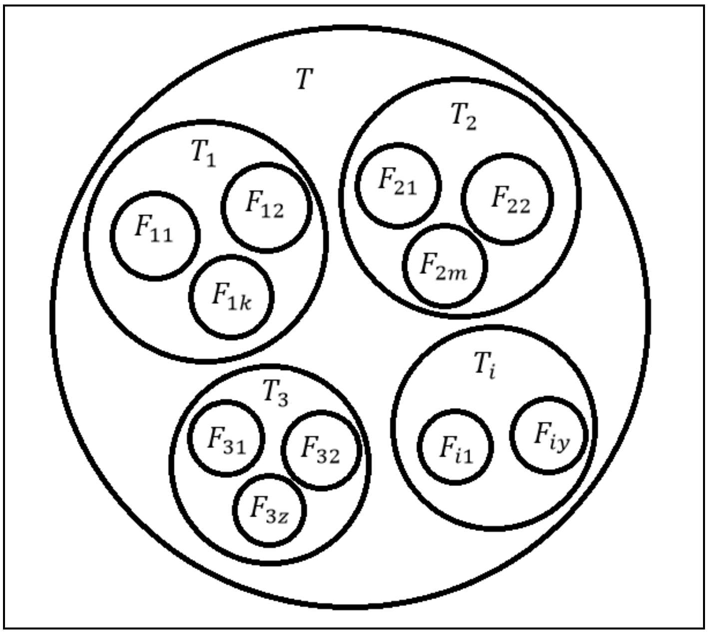


Fig. 5. Presentation of the relational data base scheme in the form of sets

Let Q be the set of all database queries provided by the business logic application:

$$Q = \{Q_l, l = 1,...m\}, \tag{3}$$

where Q_l is a *l*-th query in a set of queries *Q*;

l is a number of the query in a set of queries;

m is a total number of queries in a set of queries.

In its turn, each of the queries refers to a certain set of all database fields, i.e. each query can be represented as the following set of fields:

$$Q_l = \{F_{ij}, i \le n; j \le i_k; l = 1,...x\}, \tag{4}$$

where F_{ij} is a *j*-th field at the *i*-th table;

i is a table number in a set of tables;

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

n is a total number of tables in the scheme;

j is a field number at the i-th table;

i_k is a total field number at the i-th table;

x is a total number of queries.

The presentation of queries to the database in the form of sets is shown in fig. 6.

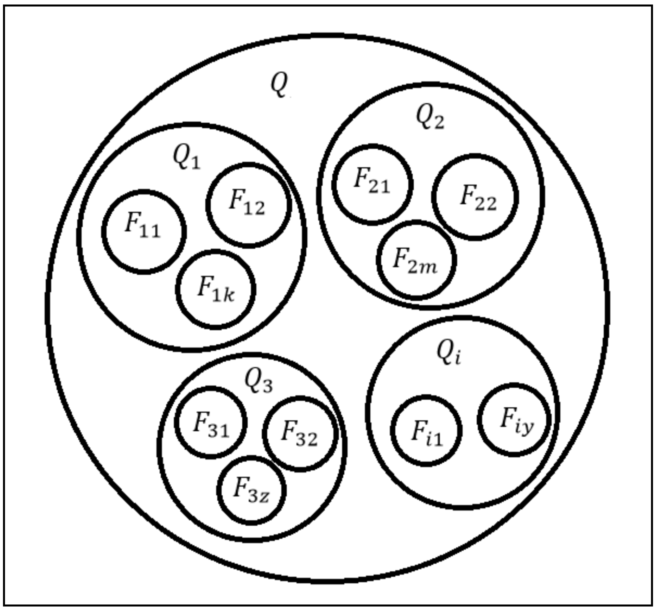


Fig. 6. Presentation of queries to the database

For each field, it is necessary to find a set of queries in which the field is used:

$$F_{ij}^{q} = \{Q_l, l = 1,...z; z \le x \mid F_{ij} \in Q_l\}, \quad (5)$$

where F_{ij}^{q} is the set of queries in which the field F_{ij} is used;

Q_l is a l-th query in which the field F_{ij} is used;

z is a number of queries in which the field F_{ij} is used;

x is a total number of queries.

At the beginning of model conversion, it is necessary to remove the fields that are not used in any query, and put these fields in a separate collection. These fields correspond to the following conditions:

$$\left|F_{ij}^{q}\right| = 0; \quad (6)$$

All such fields can be included into one (or several) collection $C_1\,(C_1 \ldots C_k)$. In the set representation this collection looks like this:

$$C_1 = \{F_{ij}, i \le n; j \le i_k \mid \left|F_{ij}^{q}\right| = 0\}, \quad (7)$$

where F_{ij} is a j-th field at the i-th table;

i is a table number in a set of tables;

n – total number of tables in the scheme;

j – number of the field at the i-th table;

i_k – total number of the fields at the i-th table.

At this stage, several collections are created if the fields falling into the above category are not connected in any way and cannot be combined into one collection from the point of view of the logical representation of the data schema.

Next, it is necessary to select those fields that take part in only one query:

$$\left|F_{ij}^{q}\right| = 1; \quad (8)$$

Fields satisfying the above condition are part of the new collection Cz:

$$C_z = \{F_{ij}, i \le n; j \le i_k \mid F_{ij} \in Q_l \,\&\, \left|F_{ij}^{q}\right| = 1\}, z > 1, \quad (9)$$

where F_{ij} – j-th field at the i-th table;

n is a total number of tables in the scheme;

i_k – total number of fields at the i-th table;

Q_l – l-th query;

F_{ij}^{q} – the set of queries in which the field F_{ij} is used;

z – collection number.

The same as for the previous set, more than one collection can be created if the fields are not linked and logically cannot be combined into one collection.

At this stage, remove by consideration those fields that have already been used in previous collections.

Let's make a set of queries H, which we will work with next, by extracting from the general set of all queries those queries, all fields of which already belong to the found collections.

Let us make even sections of the sets $Q_l \in H$, these sections have the following form:

$$Q_k^{'} = Q_i \cap Q_j;\, j \ne i;\, i, j = 1,...\left|H\right|, \quad (10)$$

where $Q_k^{'}$ is the k-th pairwise section;

H is a set of queries that are considered;

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

Q_i, Q_j – *i*-th and *j*-th query sets.

The resulting non-empty sets form a new set *M*. Provided that *H* – *M* ≠ Ø, the new collection will consist of the fields included in this difference:

$$C_g = \{F_{ij}, i \le n; j \le i_k \mid F_{ij} \in (H - M)\}, \quad (11)$$

where C_g is a new collection;

H – set of queries under consideration;

M – set of non-empty intersections;

F_{ij} – field from difference *H* – *M*.

From the set of fields taken for consideration we remove those that are included in the above set. After receiving the collection we will re-recognize the set *H* to continue the algorithm:

$$H = M, \quad (12)$$

where *H* – set of queries to be considered;

M – set of non-empty intersections.

Now we find the intersection of the fields of queries, but already 3 elements:

$$Q_k^{''} = Q_i \cap Q_j \cap Q_m; j \ne i; i, j, m = 1, \ldots |H|, \quad (13)$$

where $Q_k^{''}$ – *k*-th intersection of three elements;

H – set of queries under consideration;

Q_i, Q_j, Q_m – *i*-th, *j*-th and *m*-th sets of queries.

Similarly, as with two elements, the resulting nonvoid sets form a new set *M* and if *H* – *M* ≠ Ø, a new collection (11) is formed. Thus, the algorithm is repeated until only one intersection is left at a certain step, that is, the set H will not consist of one element, when this condition is reached, it is necessary to form a new set consisting of fields that entered the last intersection and are not included in all previous collections.

Thus, as a result of the method, a set of collections of documents with their field sets will be formed.

In further research, it is planned to compare such an algorithm for migration between data models and other algorithms on real database examples and to investigate its effectiveness

Algorithm development

The migration support algorithm is represented by means of the UML activity diagram in fig. 7.

The preparatory step for a relational model database migration algorithm to a query-based document-oriented model is to define a set of queries to the database. It is suggested to use one of the query definition options for the algorithm:

- for commercial projects, in most cases, in addition to the schema database itself, the queries to this database that are operated by the application are also known, in which case known queries are taken for the algorithm;

- if the set of queries is unknown, it is reasonable to make a deeper analysis of the subject area and the database schema and to independently compose the queries that are most likely to cover the business logic of the subject area and the application where the database is or can be used;

- if the previous two options cannot be used in a particular situation, it is proposed to consider the links between the tables as queries.

After defining a set of queries, it is necessary, using set theory, to work with the representation of tables and queries for the further work of the algorithm, namely:

- represent each table as a set of fields;

- represent each query as a set of fields used in it (in any part: sampling, grouping, etc.);

- represent each field as a set of queries in which it takes part.

If at this stage the presence of such fields that do not participate in any of the queries are detected, it is necessary to combine them into one collection (or several collections, if the business logic does not allow combining these fields into one collection) of links between the initial tables, possibly with different degrees of nesting.

The next step in the algorithm is to make links between sets of fields in queries, starting with pairwise links. For each query, i.e. set of its fields, a search for pairwise relations with all other sets of query fields is performed. If the next section is not an empty set, you must add queries from the section to the set of non-empty sections. Thus, all the paired sections are traversed and the queries from the next section are either attached or not attached to the set of non-empty sections (if a certain query is already contained in the resulting set of non-empty sections, it does not need to be added to the second set).

At the end of the formation of the resulting set of non-empty intersections, it is necessary to find the difference of the set of all queries considered at this stage (in pairs intersections - the whole set of queries) and the set of queries that entered the set of non-empty intersections. If the found difference is not an empty set, then the resulting difference is a new collection (it must be further checked that each field is included in this difference once, if there are more than one occurrence, then remove repeating fields). Also, as with the formation of the first collection, it is necessary to pay attention to the connections between the initial tables, and, if necessary, to form different degrees of the nesting of the newly created collection.

For the next step, it is necessary to override the set of queries under consideration by the set of non-empty intersections of queries obtained in the previous step.

Similarly, to the actions with pairwise sections, it is necessary to determine the set of non-empty sections queries (without repeating elements in the resulting set). Having obtained the resulting set of non-empty sections, you should find the difference between the sets of queries considered at this step and the current set of non-empty sections. If the found difference is not an empty set, then the resulting difference makes a new collection (taking into account the links between the initial tables, business logic, formalizing the necessary levels of nesting in the collection, etc.).

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

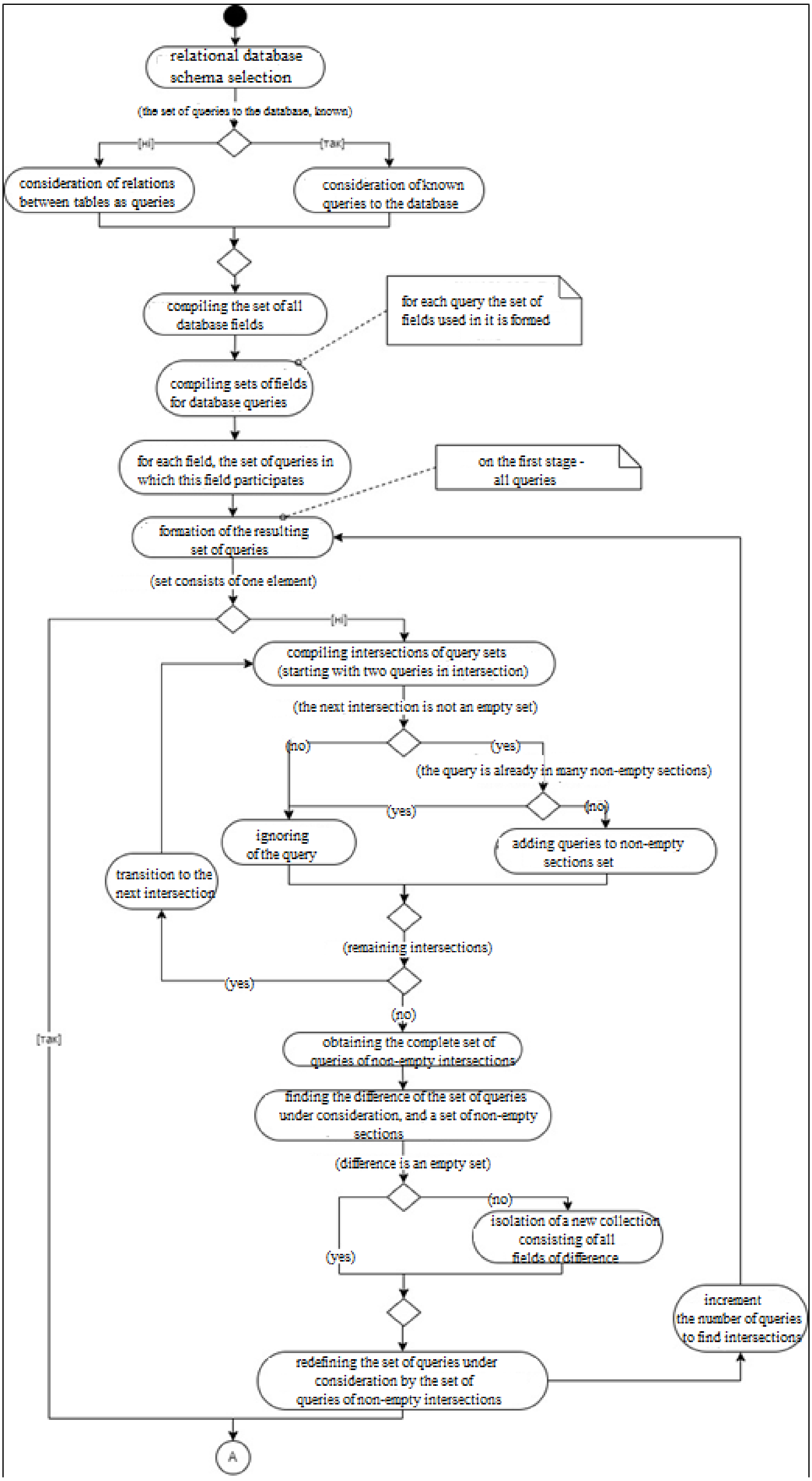


Fig. 7. UML-activity diagram for the algorithm

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

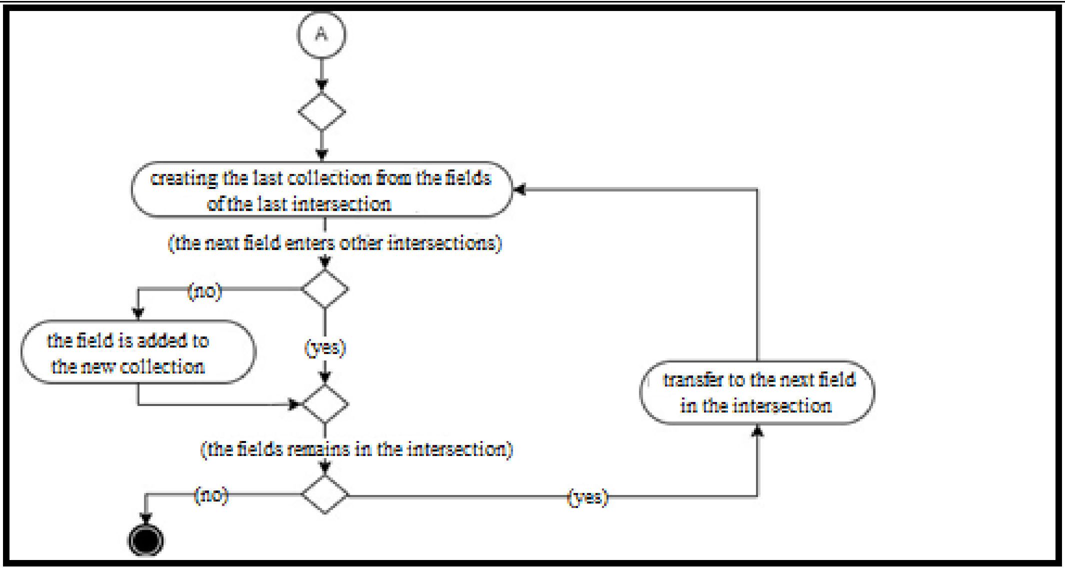


Fig. 7. Sheet 2

Similar actions to form new collections with an incremental number of queries to intersect at each step, are repeated until there remains one element in the set of queries considered at a particular step - that is, one query, and since with this query is no longer possible to build a cross section, the transition to the next stage of the algorithm. In this step, each field is checked from the set of fields of this query and, if this field does not yet belong to any of the collections created during the previous work of the algorithm, it is added to the last collection.

Thus, after the algorithm finishes, all fields are distributed among the collections in the newly created document-oriented data model.

Discussion of the results

To automate the migrations, the software was developed in the programming language C#, on the platform .NET Core. This software inputs a MS SQL relational database and a set of queries to that database, converts the database schema according to the algorithm described in this study, shows the result and creates a MongoDB database after confirmation by the user. After the successful creation of collections, the process of data transfer on the corresponding fields takes place. Such a process was run on a test database, after the migration was completed, it was verified that the data was migrated in full and without corruption. The results of query execution in the target database were also tested and matched the results obtained on the source database. Such results prove that the algorithm obtained in the study is workable and can be used for heterogeneous model-heterogeneous data migration between relational and document-oriented storage models.

Conclusions

As a result of the study it was:

- reviewed the theoretical aspects of data migration, related terms and processes;

- analyzed the popularity and relevance of using non-relational databases, on the basis of this analysis non-relational document-oriented storage model (using MongoDB as an example) was selected for consideration as a target database when migrating from the relational model;

- an analytical review of existing methods and strategies for migration between relational models and document-oriented data storage models was performed, features of such methods, limitations of such methods, cases of expediency of use and disadvantages of such methods were given;

- the possibility of using relational algebra and set theory in the context of data and query models, as well as in redesigning models was considered;

- selected a data model migration strategy that involves redesigning the database schema in accordance with database queries;

- a mathematical model for an algorithm for heterogeneous model-inhomogeneous data migration between relational and document-oriented data storage models using set theory has been compiled

- formalized and described an algorithm for data migration according to the principles of the aforementioned strategy (data query-oriented strategy).

The obtained algorithm is suitable for use on real examples, and is also an object for further research and possible improvements, analysis of efficiency in comparison with other methods.

References

1. "International Roadmap for Devices and Systems. More Moore White Paper", available at: https://irds.ieee.org/images/files/pdf/2016_MM.pdf (last accessed: 25.03.2022).
2. Morris, J. (2012), *Practical Data Migration*, BCS, The Chartered Institute for IT, London, 266 p.
3. "Homogeneous vs Heterogeneous migration", available at: https://rtfm.co.ua/aws-database-migration-service-obzor-i-primer-migracii-self-hosted-mariadb-v-aws-aurora-rds/#Homogeneous_vs_Heterogeneous_migration (last accessed: 30.03.2022).

4. Preston, Z. (2021), *Practical Guide to Large Database Migration*, CRC Press, USA, 198 p.
5. Andreas, M. (2015), "Providing Database Migration Tools. A Practitioner's Approach", *21st International Conference on Very Large Data Bases (VLDB)*, P. 635 – 641.
6. Ji, L. F., Azmi, N. F. M. (2020), "The development of a new data migration model for NOSQL databases with different schemas in environment management system", *Journal of Environmental Treatment Techniques*, No. 8 (2), P. 787–793.
7. Ceresnak, R., Dudas, A., Matiasko, K. (2021), "Mapping rules for schema transformation : SQL to NoSQL and back", *International Conference on Information and Digital Technologies*, P. 52–58. **DOI**: https://doi.org/10.1109/IDT52577.2021.9497629
8. Hanine, M., Bendarag, A., Boutkhoum, O. (2015), "Data Migration Methodology from Relational to NoSQL Databases", *International Journal of Computer, Electrical, Automation, Control and Information, Engineering*, No. 9 (12), P. 2566–2570.
9. Alalfi, M. H. (2018), "Automated Algorithm for Data Migration from Relational to NoSQL Databases", *Al-Nahrain Journal for Engineering Sciences (NJES)*, No. 21 (1), P. 60–65. **DOI**: https://doi.org/10.29194/NJES2101
10. Fouad, T., Mohamed, B. (2019), "Model transformation from object relational database to NoSQL document database", *NISS19*, No. 49, P. 1–5. **DOI**: https://doi.org/10.1145/3320326.3320381
11. Li, X., Ma, Z., Chen, H. (2014), "QODM: A Query-Oriented Data Modeling Approach for NoSQL Databases", *IEEE Workshop on Advanced Research and Technology in Industry Applications*, P. 338–345.
12. Alotaibi, O., Pardede, E. (2019), "Transformation of Schema from Relational Database (RDB) to NoSQL Databases", *Data*, No. 4 (4), P. 148. **DOI**: https://doi.org/10.3390/data4040148
13. Ain El Hayat, S., Bahaj, M. (2020), "Modeling and transformation from temporal object relational database into mongodb: Rules", *Advances in Science, Technology and Engineering Systems*, No. 5 (4), P. 618–625. **DOI**: https://doi.org/10.25046/aj050473
14. Mason, R. T. (2015), "NoSQL databases and data modeling techniques for a document-oriented NoSQL database", *Informing Science & IT Education Conference (InSITE)*, P. 259–268. **DOI**: https://doi.org/10.28945/2245
15. Alekseev, A. A., Osipova, V. V., Ivanov, M. A. (2016), "Efficient data management tools for the heterogeneous big data warehouse", *Physics of Particles and Nuclei Letters*, No. 13 (5), P. 689–692. **DOI**: https://doi.org/10.1134/S1547477116050022
16. Gu, Y., Wang, X., Shen, S., Wang, J., Kim, J.-U. (2015), "Analysis of data storage mechanism in NoSQL database MongoDB", *2015 IEEE International Conference on Consumer Electronics*, P. 158–159.
17. Dabowsa, N. I., Maatuk, A. M., Elakeili, S. M. (2021), "Converting Relational Database to Document-Oriented NoSQL Cloud Database", *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, P. 381–386. **DOI**: https://doi.org/10.1109/MI-STA52233.2021.9464488
18. Date, C. J. (2012), *SQL and Relational Theory: How to Write Accurate SQL Code*, O'Reilly Media, London, 448 p.
19. Kuzochkina, A., Shirokopetleva, M., Dudar, Z. (2018), "Analyzing and Comparison of NoSQL DBMS", *International Scientific-Practical Conference on Problems of Infocommunications Science and Technology*, P. 560–564. **DOI**: https://doi.org/10.1109/INFOCOMMST.2018.8632133

"DB-Engines Ranking", available at: https://db-engines.com/en/ranking (last accessed: 10.04.2022).

20. Chickerur, S., Goudar, A., Kinnerkar, A. (2015), "Comparison of Relational Database with Document-Oriented Database (MongoDB) for Big Data Applications", *8th International Conference on Advanced Software Engineering & Its Applications (ASEA)*, P. 41–47. **DOI**: https://doi.org/10.1109/ASEA.2015.19
21. Stepovik, A. N, Efanov, N. V. (2019), "Analysis of relational and non-relational databases", *Digitization of the economy: directions, methods, tools*, P. 414–416.

Received 13.04.2022

Відомості про авторів / Сведения об авторах / About the Authors

Перетятко Марія Вікторівна – Харківський національний університет радіоелектроніки, магістрант кафедри програмної інженерії, Харків, Україна; e-mail: mariia.peretiatko@nure.ua; ORCID ID: https://orcid.org/0000-0003-3711-3765. Моб. 0995455388.

Перетятко Мария Викторовна – Харьковский национальный университет радиоэлектроники, магистрант кафедры программной инженерии, Харьков, Украина.

Peretiatko Mariia – Kharkiv National University of Radio Electronics, undergraduate at the Department of Software Engineering, Kharkiv, Ukraine.

Широкопетлєва Марія Сергіївна – Харківський національний університет радіоелектроніки, старший викладач кафедри програмної інженерії, заступник директора центра післядипломної освіти, Харків, Україна; e-mail: marija.shirokopetleva@nure.ua; ORCID ID: https://orcid.org/0000-0002-7472-6045. Моб. 0664039164.

Широкопетлева Мария Сергеевна –Харьковский национальный университет радиоэлектроники, старший преподаватель кафедры программной инженерии, заместитель директора центра последипломного образования, Харьков, Украина.

Shirokopetleva Mariia – Kharkiv National University of Radio Electronics, senior lecturer at the Department of Software Engineering, Deputy Director of the Center for Postgraduate Education, Kharkiv, Ukraine.

Лєсна Наталя Совєтівна – кандидат технічних наук, професор, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, м.Харків, Україна; email: natalya.lesna@nure.ua; ORCID ID: https://orcid.org/0000-0001-9816-3251. Моб. 0633516752.

Лесная Наталья Советовна – кандидат технических наук, профессор, Харьковский национальный университет радиоэлектроники, профессор кафедры программной инженерии, г.Харьков, Украина; email:natalya.lesna@nure.ua

Lesna Natalya – Candidate of Technical Sciences (Ph.D.), Professor, Kharkiv National University of Radio Electronics, Professor at the Department of Software Engineering, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДТРИМКИ МІГРАЦІЙ ДАНИХ МІЖ РЕЛЯЦІЙНИМИ І ДОКУМЕНТНИМИ МОДЕЛЯМИ ЗБЕРІГАННЯ ДАНИХ

Предметом дослідження в статті є гетерогенна модельно-неоднорідна міграція даних між реляційними та документо-орієнтовними моделями зберігання даних, існуючі стратегії та методи підтримки такого роду міграцій, використання реляційної алгебри та теорії множин у контексті баз даних при побудові нового алгоритму міграції даних. **Мета** роботи – розглянути особливості та порядок міграції даних, дослідити методи підтримки міграції даних між реляційними і документними моделями даних, побудувати математичну модель та алгоритм для міграції даних. Використовуються такі **методи:** аналіз та порівняння існуючих підходів до міграції даних, вибір стратегії для подальшого використання при складанні алгоритму міграції, математичне моделювання алгоритму гетерогенної модельно-неоднорідної міграції даних, формалізація алгоритму міграції даних. В статті вирішуються наступні **завдання:** розгляд поняття та різновидів міграції даних, обґрунтування вибору документо-орієнтовної моделі даних в якості цільової для міграції даних, аналіз існуючих літературних джерел, що стосуються методів та стратегій гетерогенної неоднорідно-модельної міграції даних з реляційної до документо-орієнтовної моделі даних, виділення переваг та недоліків існуючих методів, вибір підходу до формування алгоритму міграції даних, складання та опис математичної моделі міграції даних за допомогою реляційної алгебри та теорії множин, представлення алгоритму міграції даних, в основі якого лежить орієнтація на запити до даних. Отримано наступні **результати:** використано можливості реляційної алгебри і теорії множин у контексті моделей даних та запитів, а також при перепроектуванні моделей, обрано стратегію міграції моделей даних, яка передбачає перепроектування схеми бази даних у відповідності до запитів до бази даних, створено математичну модель методу гетерогенної неоднорідно-модельної міграції між реляційною та документо-орієнтовною моделями даних, описано алгоритм застосування цього методу. **Висновки:** в результаті проведеної роботи проаналізовано основні методи підтримки міграції для різних моделей зберігання даних, за допомогою реляційної алгебри та теорії множин побудовано математичну модель та складено алгоритм перетворення реляційної моделі даних до документо-орієнтовної моделі даних з урахуванням запитів до даних. Отриманий алгоритм є придатним для використання на реальних прикладах, а також є об’єктом для подальших досліджень і можливих удосконалень, аналізу ефективності у порівнянні з іншими методами.

Ключові слова: база даних; гетерогенна міграція; модель даних; теорія множин.

ИССЛЕДОВАНИЕ МЕТОДОВ ПОДДЕРЖКИ МИГРАЦИЙ ДАННЫХ МЕЖДУ РЕЛЯЦИОННЫМИ И ДОКУМЕНТНЫМИ МОДЕЛЯМИ ХРАНЕНИЯ ДАННЫХ

Предметом исследования в статье является гетерогенная модельно-неоднородная миграция данных между реляционными и документо-ориентированными моделями хранения данных, существующие стратегии и методы поддержки такого рода миграций, использование реляционной алгебры и теории множеств в контексте баз данных при построении нового алгоритма миграции данных. **Цель** работы – рассмотреть особенности и порядок миграции данных, исследовать методы поддержки миграции между реляционными и документными моделями данных, построить математическую модель и алгоритм для миграции данных. Используются следующие **методы:** анализ и сравнение существующих подходов к миграции данных, выбор стратегии для дальнейшего использования при составлении алгоритма миграции, математическое моделирование алгоритма гетерогенной модельно-неоднородной миграции данных, формализация алгоритма миграции данных. В статье решаются следующие **задачи:** рассмотрение понятия и разновидностей миграции данных, обоснование выбора документо-ориентированной модели данных в качестве целевой для миграции данных, анализ существующих литературных источников, касающихся методов и стратегий гетерогенной неоднородно-модельной миграции данных из реляционной к документо-ориентированной модели данных существующих методов, выбор подхода к формированию алгоритма миграции данных, составление и описание математической модели миграции данных с помощью реляционной алгебры и теории множеств, представление алгоритма миграции данных, в основе которого лежит ориентация на запросы к данным. Получены следующие **результаты:** использованы возможности реляционной алгебры и теории множеств в контексте моделей данных и запросов, а также при перепроектировании моделей, выбрана стратегия миграции моделей данных, предусматривающая перепроектирование схемы базы данных в соответствии с запросами к базе данных, создана математическая модель метода гетерогенной неоднородно-модельной миграции между реляционной и документо-ориентированной моделями данных, описан алгоритм применения этого метода. **Выводы:** в результате проведенной работы проанализированы основные методы поддержки миграции для различных моделей хранения данных, с помощью реляционной алгебры и теории множеств построен математическая модель и составлен алгоритм преобразования реляционной модели данных в документо-ориентированную модель данных с учетом запросов к данным. Полученный алгоритм пригоден для использования на реальных примерах, а также является объектом для дальнейших исследований и возможных усовершенствований, анализа эффективности по сравнению с другими методами.

Ключевые слова: база данных; гетерогенная миграция; модель данных; теория множеств.

Бібліографічні описи / Bibliographic descriptions

Перетятко М. В., Широкопетлєва М. С., Лєсна Н. С. Дослідження методів підтримки міграцій даних між реляційними і документними моделями зберігання даних. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 64–74. DOI: https://doi.org/10.30837/ITSSI.2022.20.064

Peretiatko M., Shirokopetleva M., Lesna N. (2022), "Research of methods to support data migration between relational and document data storage models", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 64–74. DOI: https://doi.org/10.30837/ITSSI.2022.20.064

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

JEL J30, J31, C10 DOI: https://doi.org/10.30837/ITSSI.2022.20.075

L. MALYARETS, O. IASTREMSKA, A. TUTOVA

DETERMINATION OF PRIORITY QUALITATIVE FACTORS OF STIMULATION OF THE WORK OF ENTERPRISE TOP MANAGERS

The article is devoted to substantiation of the main subjective qualitative factors which are typical for labor incentives of managers of the strategic level of enterprises management, and which it is reasonable to take into account while developing the system of economic incentives of their activity, since basing and determination of the incentives amount only on the statistical objective information is not able to influence significantly the final results of top-managers work. The **purpose** of the article is to identify priority qualitative factors of influence on the process of economic stimulation of the activity of top managers of industrial enterprises and their quantitative interpretation based on the combination of qualitative assessments into an integral indicator. The **tasks** of the article are the analysis of the results of the survey of top managers on individual qualitative factors of influence on their motivation, the definition of statistical relationships between factors, determining the explicit and latent trends in the dynamics of these factors, the calculation of the integral indicator of the impact of the identified significant factors, the formation of methodological support to identify priority qualitative factors of economic incentives performance of top managers of industrial enterprises. The **object** of the article is the process of economic stimulation of the results of activity of top managers of industrial enterprises. The **subject** of the article is the theoretical provisions, methodological support, and practical proposals for economic incentives for managers of the strategic level of administration at industrial enterprises. **Methods.** To achieve the goal, the article used the following basic general and special research methods: theoretical generalization, questionnaire survey, descriptive statistics tools, Spearman rank correlation coefficient, multivariate factor analysis, method for calculating the integral index of qualitative factors of managers' labor stimulation, graphical method. **Results.** The results of the study are: the scientific achievements of the predecessors on the formation and use of performance indicators of enterprises as indicators of incentives for top managers; surveyed top managers of industrial enterprises regarding their opinions on the main factors influencing the performance of their own activities; proved the relationship of influence factors on the incentives of top managers presented in the questionnaire; clear and latent tendencies of interrelation of factors of influence on productivity of managers of strategic level of the enterprises are revealed; the integrated indicator of qualitative factors of stimulation of work of managers is defined, quantitative values of which have proved existence of insufficient account of factors on process of stimulation. **Conclusions.** As a result of determining the relationship between the qualitative factors influencing the economic incentives of top managers developed methodological support, which differs: the content of qualitative factors; analysis of the structure of the studied set of arrangements of answers of experts using the tools of descriptive statistics; assessment of the closeness of the relationship between qualitative factors of economic incentives for top managers in the dynamics; assessment of the consistency of the answers of experts in the dynamics; identification of latent factors of economic stimulation of top managers; analytical method of developing an integrated quality indicator of economic stimulation for top managers.

Keywords: stimulation of labor; top manager; industrial enterprise; qualitative factors; the relationship between the qualitative factors; methodological support.

Introduction

The success of enterprise activity depends on many factors, among which there are objective, such as efficiency of economic resources use, qualification of workers, organization of production processes, and subjective, connected with human perception of events, interest of workers, their motivation and used incentive systems, validity of rewards, criterion indicators of their purpose If objective factors are studied widely enough, then subjective factors are given me Research concerning the development of proposals on the formation and use of incentive systems for production personnel is more widespread, while almost no attention is paid to the stimulation of managers, especially strategic level managers. Economic stimulation of this category of personnel is usually connected only with an enterprise profit and other indices of its finite activity. Therefore, there is an objective necessity in development of the system of stimulation of top managers and their building not only on traditional indicators, but also on the indicators of qualitative type having subjective nature.

Analysis of publications

In the works of many scientists [1, 8 - 13] it is noted that in modern conditions stimulation of top managers' work is one of the determining functional components of enterprise management and its development. This is explained by the increasing role of the human factor in ensuring the company's competitiveness, its effective activity both on internal markets and on external ones [8, 12]. Formation of the mechanism of motivation and economic stimulation of personnel will have a positive impact on labor efficiency, and it will be reflected in all business processes and results of enterprise activity, and, consequently, will allow increasing its profitability and profitability.

In the organization and implementation of economic stimulation of top managers' work, an important role is played by the assessment of their work. Scientists note [9, 10] that personnel assessment in the system of economic stimulation should be performed taking into account the action of objective laws that regulate an employee's behavior. This is pointed out by the vast majority of scientists, for example, T. Momot, etc. [17]. At the same time, the authors [14] consider the presence of technological competences and their social responsibility in relation to their subordinates to be important features of managers' labor stimulation. Researchers in their work [15] suggest that in order to motivate managers their management style should be evaluated, which should correspond to a certain situation at an enterprise. At the same time, it is advisable to adapt the management style to the goals of the enterprise, its chosen strategy [16]. Moreover, according to the achieved results of the strategy to stimulate enterprise managers depending on their personal contributions to the achieved results. To provide effective economic stimulation of personnel based on its assessment at all levels of economic structure the assessment mechanism should be carried out on the principles of universality, consistency, comprehensiveness, fairness, comparison [1]. It causes the objective necessity to determine the qualitative factors of economic stimulation of top managers' work, which causes the necessity to formulate such purpose of the article, its object and subject.

The aim of the article is to identify priority qualitative factors of influence on the process of economic stimulation of activity of top managers of industrial enterprises and their quantitative interpretation based on qualitative assessments into an integral indicator. The object of the article is the process of economic stimulation of the performance of top managers of industrial enterprises. The subject of the article is the theoretical provisions, methodological support, and practical proposals for economic incentives for managers of the strategic level of administration of industrial enterprises.

Specialists in solving the problems of economic stimulation of personnel labor believe that wages cannot be the only goal of labor activity and speak about the system of economic stimulation. The system of economic stimulation of top managers at an enterprise should be based on the following basic principles [2]:

- communication, cooperation and agreement between the top managers and the management of the enterprise on the general principles of the system;
- a substantiated system of performance evaluation of top managers and definition of its indicators;
- substantiated and established criteria for defining and evaluating the work of top managers;
- substantiated standards, their control and periodic revision;
- a clear coordination of economic stimulation of top managers with the performance of the enterprise;
- material incentives, especially additional ones, not for the level of performance in general, but precisely for the achievement of qualitative results of activity.

Consequently, it is necessary to take a systematic approach to economic incentives for top managers, implementing seven key steps, namely: identification of economic problems of the enterprise arising from the lack of economic incentives and expressed in low labor efficiency, staff turnover, an unfriendly atmosphere within the team; making a list of key objectives of the enterprise, involving an increase in labor productivity, raise the team spirit, the formation of a cohesive team; conducting social diagnostics based on a questionnaire survey, as a result of which material and non-material stimuli are specified, which are needed both for each individual top manager and for their entire team; based on the results of social diagnostics, developing a sequence of economic stimulation measures; determining financial costs for implementing measures of economic stimulation of top managers; informing top managers on the implementation of measures of economic stimulation system for detailed information about charges in the bonus system; approbation of this system of economic stimulation of labor of top managers and establishment of the ratio between costs and received profit from implementation of measures, and further elimination of troubles and problems that have appeared in the process of implementation [3].

Despite the significant amount of works of famous specialists, many issues of economic stimulation of labor of top managers remain unsolved and insufficiently grounded; it concerns both understanding of the process of economic stimulation itself, as well as peculiarities of forming forms, methods, and recommendations on improvement of the economic stimulation of labor at enterprises.

Leshchenko L.O. recommends apart from direct and indirect economic stimulation to distinguish social motivation, when an employee understands that he is part of the team; psychological motivation, when a friendly and welcoming atmosphere is observed in the team; career motivation, when conditions for career growth exist in the team; educational motivation, when employees are interested in training and development [4].

Research results

Among the factors of economic stimulation of top managers' labor, a special place is held by qualitative factors that take into account the behavior, personal expectations, perceptions and values of each individual. Consideration of qualitative factors of economic stimulation of top managers' labor is carried out through the study of qualitative features of their activity, namely: rational and emotional components of activity; special and typical behavioral patterns of top managers; identification of unrealized needs in the process of activity; development of new methods of material stimulation. Quantitative factors are based on a rational approach to economic stimulation, and qualitative factors take into account each individual's motivation, unique social experience, his abilities and many other features of this subject that make up his "life world". Exactly qualitative factors of economic stimulation of top managers are directed on the clarification of subjective-specific factors of activity, on understanding of those moments, which the staff is guided in its activity.

It should be noted that many scientists believe that in order to improve the overall effectiveness of the enterprise, in addition to material stimulation, there is the implementation of qualitative factors of economic stimulation of work of top managers, namely, such factors as term of employment as a top manager, the level of compensation for increased economic stimulation of labor, satisfaction with the existing system of economic stimulation at the enterprise, the level of compensation, the main economic stimulating factor of labor, factor of current material rewards, current factor of influence on the receipt of monetary compensation, negative factors

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

affecting the bonus system at the enterprise These qualitative factors will increase organizational loyalty, responsibility, and willingness to work more efficiently. The purpose of considering qualitative factors is to increase:

- employee satisfaction by obtaining greater economic stimulation of top managers' work;
- needs of employees in growth, development and self-expression by means of getting higher satisfaction with existing system of economic stimulation at the enterprise;
- team building based on the increase of the existing material rewards;
- commitment of employees to work, striving to achieve the general corporate goals due to the main economic stimulating factor of labor;
- striving for training and development of the personnel potential on the basis of improvement of the bonus system at the enterprise.

Consequently, to increase the level of economic incentives for top managers and determine the qualitative factors it is necessary to develop a questionnaire, and the answers to the questions of the questionnaire will help to better understand the desire of employees, their needs, desires, with which you can implement certain changes that will reduce staff turnover and will help to attract new employees - managers of the strategic level of management. The questionnaire formed questions, the answers to which should be given in points. It is known that psychologists, sociologists, and economists have developed various methods for establishing scores for a qualitative attribute. However, almost all of them are based on the well-known studies of E. Weber, G. Fechner, S. Steven. In 1846, E. Weber formulated a law related to the stimulus of the measured value s. E. Weber's law states that a change in perception is manifested when the stimulus is increased by a constant fraction of the stimulus itself. This law is valid when Δs is small compared to s, but practically ceases to be valid when s is either very small or very large. Saaty believes that synthesizing or decomposing stimuli, traceable to clusters or levels of hierarchy, is an effective means of extending the application of this law [5, p. 68]. According to T. Saaty, we have the following explanations for measuring the essence of factor scores:

1 - equal significance (two actions contribute equally to the goal); 3 - a certain advantage of significance of one action over another (weak significance) (experience and judgment give a slight advantage of one action over another); 5 - significant or strong significance (experience and judgment give a significant advantage of one action over another); 7 - very strong or obvious significance (the advantage of one action over another is very significant. Its superiority is almost obvious); 2, 4, 6, 8 - intermediate values between adjacent values of the scale (a situation where a compromise decision is needed); inverse values of the above numbers - if action i is assigned one of the above numbers in comparison with action j, then action j is assigned an inverse value in the comparison with i (a reasonable guess); rational values - relations arising in a given scale (if consistency is postulated, then n numerical values are needed to obtain the matrix).

G. Fechner found that stimuli with noticeable differences are placed in a geometric progression, and the corresponding perceptions constitute an arithmetic progression at discrete points where barely noticeable differences are observed. Stimuli arise in the process of pairwise comparisons relative to comparative actions. The Weber-Fechner psychophysical law results in a sequence of 1, 2, 3, ... There are about five with additional ones making up the trade-offs between neighboring reactions. This increases the number of differences to nine, which is consistent with the order-of-magnitude predictions. Malyarets L.M., who also believes that it is appropriate to use the five-point system [6], gives a detailed analysis of the measurement of ordinal features in the monograph. The established points (for example, 1, 2, 3, 4, 5) are the expression of nominations of qualitative property of object (in the example: very low (1), low (2), moderate (3), strong (4), very strong (5)).

Consequently, in order to determine the priority of factors, a questionnaire was developed, in which questions were included and a survey of top managers of enterprises was conducted. At the same time, it can be considered that these top managers are experts due to their high level of professionalism, so their answers can be considered as experts' answers. The content of the questions of the questionnaire describing the main reasons for economic incentives for top managers is presented in table 1. The answers to the questions of the questionnaire are presented on a five-point scale.

Table 1. *Questionnaire questions describing the main qualitative factors of economic incentives for top managers and their scale*

No.	Question	Meaning of the value	Explanations
1	How long have you worked as a top manager? Where:	1	Less than 1 year
		2	Over 3 years
		3	Over 5 years
		4	Over 10 years
		5	5 years
2	Rate on a scale of 1-5, how does your pay level affect your economic stimulation?	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

The end **Table 1.**

3	On a scale of 1-5, are you satisfied with your economic stimulation system?	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly
4	Evaluate on a scale of 1-5, are you satisfied with your pay?	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly
5	Evaluate on a scale of 1-5, what is the most effective economic incentive for you to work?	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly
6	Evaluate on a scale of 1-5, what types of material rewards you receive most influence you?	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly
7	Evaluate on a scale of 1-5 points which factors are more influential in receiving your monetary reward.	1	very weakly
		2	weakly
		3	sufficiently
		4	significantly
		5	very strongly
8	Identify the main problems of the bonus system at your company on a scale of 1-5 points?	1	Weak link between communication goals
		2	Lack of understanding of the rewarding principles
		3	Incomprehension of the goals set
		4	Conflict (overlapping) of goals
		5	Strong conflict

The level of labor of top managers is influenced by qualitative factors, namely: the period of work in the position of a top manager (z1), the level of remuneration for increasing economic stimulation of labor (z2), satisfaction with the existing economic stimulation system at the enterprise (z3), the level of labor compensation (z4), the main economic stimulating labor factor (z5), the factor of effective material rewards (z6), the effective impact factor for monetary rewards (z7), negative factors affecting the bonus system at the enterprise (z8). The values of these qualitative factors are measured in ordinal scales. Specialists of economic and mathematical methods and data analysis in economics consider that the main tasks of the theory and practice of measuring ordinal values are: analysis of the structure of the investigated set of orderings (task A); analysis of integral (aggregate) consistency of variables and their conditional ranking by the criterion of the degree of close connection of each of them with the remaining variables (task B); construction of a single group ordering of objects on the basis of the available set of consistent orderings (task C)[6].

Therefore, the first step in determining the qualitative factors of economic incentives for the work of top managers is their description at each enterprise under study annually. To describe the qualitative factors we use the tools of descriptive statistics used for qualitative attributes measured in ordinal scales. Thus, the analysis of the structure of the studied population of ordering of experts' responses to qualitative factors of economic incentives is an important step, which is carried out by means of univariate distribution, which allows summarizing the frequency with which different values of a certain variable are observed in the data set. In addition, this is done through the operation of tabulation or cross-tabulation [6]. Thus, visualization of the characteristic of economic incentives for the work of top managers on eight qualitative factors in the Private Joint Stock Company " Kharkiv Stamp and Mold Plant" according to the opinion of 10 experts in the first year of the study is shown in fig. 1:

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

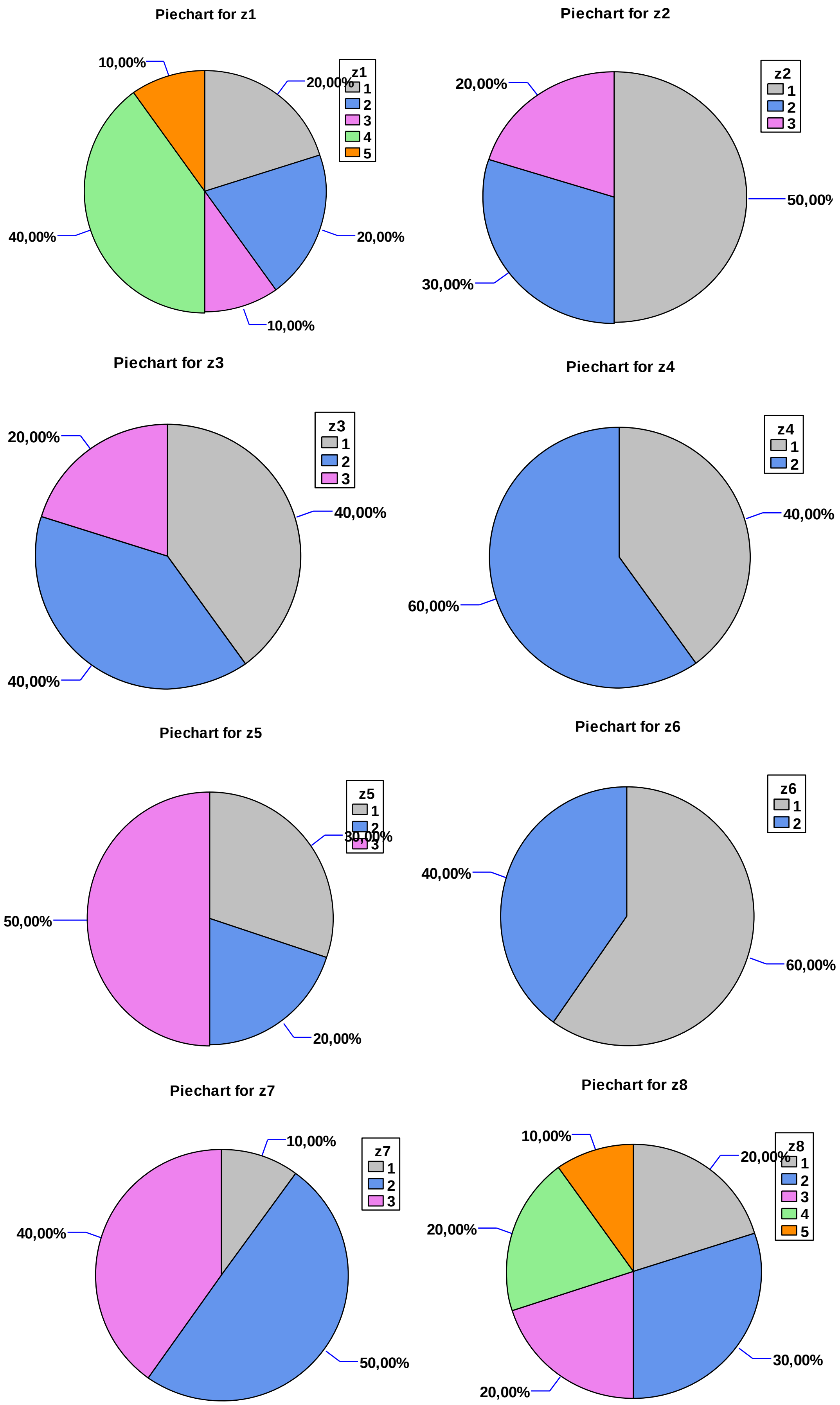


Fig. 1. Relative frequency of levels of qualitative factors of economic stimulation of the top managers of the company Private Joint Stock Company «Kharkiv Stamp and Mold Plant" in the first year of the study (in %)

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

So, the experts believe that the following situation is observed at this enterprise on economic stimulation of labor of top managers: mostly the employees have more than 10 years of work experience in the position of top manager, there is a very weak influence of salary level on the increase of economic stimulation of labor, absolutely not satisfied with the existing system of economic stimulation at the enterprise, mediocre satisfied with the level of salary, factor of the current material rewards is very weak, the factor of current material rewards is very weak, the current factor of influence on the receipt of monetary rewards is weak, among the negative factors that affect the bonus system at the enterprise is the predominant misunderstanding of the principles of bonuses.

Table 2 shows the results of the analysis of diagrams of all eight qualitative factors of economic incentives for top managers at the enterprise during the entire study period. Table 2 shows the values of qualitative factors that have the highest frequency according to experts, if there are two, the average value is indicated, as well as the value of the concordance coefficient (CC), which indicates the consistency of experts' opinions.

Table 2. *Dynamics of qualitative factors of economic stimulation of the work of top managers at the enterprise Private Joint Stock Company "Kharkiv Stamp and Mold Plant"*

Year	***Qualitative factors (z)***								***KK***
	1	2	3	4	5	6	7	8	
1	4	1	1,2	2	3	1	2	2	0,64
2	3	1	2,3	1	2	1	1	4,5	0,45
3	3,4	2	2	1	2	2,3	3	5	0,55
4	4	1,2	1	1	2	2	2	5	0,62
5	5	2,3	2	2	2	3	1	1	0,68
Average value	3,9	1,6	1,8	1,4	2,2	1,9	1,8	3,5	

Thus, at the enterprise during the whole period of the research the term of employment of the top management personnel is more than 10 years, there is also a weak impact of the level of salary on the increase of economic stimulation of labor, top managers are also weakly satisfied with the level of wages, the weak main economic incentive factor of labor, the weak factor of the current material rewards, the weak current factor of influence on the monetary reward, among the negative factors affecting the bonus system at the enterprise preferable is a conflict, that is, the inconsistency of the principles of bonuses.

Further, it is advisable to continue this analysis of the qualitative factors of economic incentives of top managers by analyzing the paired and multiple relationships in the system of factors, and therefore, it is necessary to calculate the coefficients of rank correlation. The analysis of the relationships of ordinal variables is based on different variants of probability space models, in which the role of the space of elementary results (consequences) is performed by the set of all possible combinations of n elements (n – the number of statistically studied objects). Traditionally, Spearman's or Kendel's rank correlation coefficients have been used as the main characteristics of the paired statistical relationship between orders. As we know, the first to propose a solution to the problem of testing the hypothesis of the independence of ordinal features psychologist Charles Spearman in 1900. The second most popular rank correlation coefficient, the Kendall coefficient, uses as a measure of similarity between two rankings the minimum number of permutations of neighboring objects that need to be done to transform one ordering of objects into another. In the table 3 presents the value of Spearman's correlation coefficient for assessing the closeness of the relationship of questions in the questionnaire, which characterize the main factors of economic stimulation for top managers at the enterprise Private Joint Stock Company "Kharkiv Stamp and Mold Plant".

Table 3. *The value of Spearman's rank correlation coefficient in assessing the closeness of the relationship between the questions in the questionnaire of the first year of the study*

The value of Spearman's rank correlation coefficient according to the qualitative factors of the questionnaire								
	z1	z2	z3	z4	z5	z6	z7	z8
z1		-0,2186	-0,0269	0,0369	-0,3690	-0,5904	-0,8350	-0,5692
		(10)	(10)	(10)	(10)	(10)	(10)	(10)
		0,5119	0,9356	0,9118	0,2683	0,0765	0,0122	0,0877
z2	-0,2186		0,0352	0,1543	0,1357	0,3472	0,2291	0,2622
	(10)		(10)	(10)	(10)	(10)	(10)	(10)
	0,5119		0,9159	0,6434	0,6839	0,2976	0,4918	0,4315
z3	-0,0269	0,0352		-0,3043	-0,3240	0,2282	-0,1076	0,5635
	(10)	(10)		(10)	(10)	(10)	(10)	(10)
	0,9356	0,9159		0,3613	0,3311	0,4936	0,7469	0,0909
z4	0,0369	0,1543	-0,3043		-0,5015	-0,1667	0,3536	-0,0726
	(10)	(10)	(10)		(10)	(10)	(10)	(10)
	0,9118	0,6434	0,3613		0,1325	0,6171	0,2888	0,8275
z5	-0,3690	0,1357	-0,3240	-0,5015		0,3086	-0,0764	0,1378
	(10)	(10)	(10)	(10)		(10)	(10)	(10)
	0,2683	0,6839	0,3311	0,1325		0,3545	0,8188	0,6792

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

The end **Table 3.**

z6	-0,5904	0,3472	0,2282	-0,1667	0,3086		0,3536	0,8352
	(10)	(10)	(10)	(10)	(10)		(10)	(10)
	0,0765	0,2976	0,4936	0,6171	0,3545		0,2888	0,0122
z7	-0,8350	0,2291	-0,1076	0,3536	-0,0764	0,3536		0,3595
	(10)	(10)	(10)	(10)	(10)	(10)		(10)
	0,0122	0,4918	0,7469	0,2888	0,8188	0,2888		0,2808
z8	-0,5692	0,2622	0,5635	-0,0726	0,1378	0,8352	0,3595	
	(10)	(10)	(10)	(10)	(10)	(10)	(10)	
	0,0877	0,4315	0,0909	0,8275	0,6792	0,0122	0,2808	

Consequently, in the first year of the study, the current material rewards factor (z6) and the negative factors affecting the bonus system at the company (z8), as well as the period of employment as a top manager (z1) and the current influence factor on monetary rewards (z7) are closely correlated. The analysis of the calculated Spearman correlation coefficients between the factors of economic stimulation of top managers at the enterprise Private Joint Stock Company " Kharkiv Stamp and Mold Plant" during the rest of the study showed that there are such close relationships between qualitative factors of economic stimulation of top managers, namely: $z_6 \leftrightarrow z_8$, $z_1 \leftrightarrow z_7$, $z_7 \leftrightarrow z_8$, $z_2 \leftrightarrow z_3$, $z_2 \leftrightarrow z_6$, $z_1 \leftrightarrow z_8$, $z_3 \leftrightarrow z_5$, $z_3 \leftrightarrow z_6$, $z_2 \leftrightarrow z_4$, $z_6 \leftrightarrow z_7$. We have that in the system of qualitative factors of economic stimulation of top managers' labor the most closely correlated are the factor of effective material rewards (z6), negative factors influencing the bonus system at the enterprise (z8), the acting factor of influence on monetary rewards (z7), and the factor of satisfaction with the existing system of economic stimulation at the enterprise (z3).

Using the mathematicians' proof that Spearman's rank correlation coefficient coincides with the usual Pearson's pair correlation coefficient calculated by ranks [6], multivariate factor analysis, further factor analysis, can be used for the data measured in ordinal scales. This allows us to use factor analysis to unambiguously determine the level of qualitative factors of economic stimulation of the top managers' labor to develop an integral indicator, taking into account the relationship between them. It is known that in modern mathematical statistics, factor analysis is understood as a set of methods, which, based on the existing relationships of the characteristics of the object, allow us to identify the latent generalizing characteristics. First, there is a set of elementary characteristics of the object xj, the interaction of which implies the presence of certain causes, that is, the presence of some latent factors. The latter are established as a result of the generalization of elementary attributes and act as integrated characteristics or attributes, but more complex, of a higher level. It should be noted that not only trivial attributes xj, but also the observed objects Ni can correlate, so the search for latent factors is theoretically possible by both attributes and object data [13]. Since factor analysis makes it possible to compress the initial system of indicators to a smaller number of generalizing attributes, it should be used to develop a qualitative integral indicator of economic stimulation of top managers' labor.

Table 4 presents the definition of the number of significant latent factors to describe the initial system of qualitative signs of economic stimulation of the top managers' labor at the enterprise.

Table 5 shows the factor loadings of qualitative attributes of economic stimulation of the top managers' labor in the enterprise after the turn of VARIMAX, which provides a simpler structure of latent factors.

Table 4. *Percentage of variation explained by selected latent factors*

Factor number	Own value of the factor	Dispersion value of the factor, %	Value of cumulative, accumulated dispersion, %
1	1,94154	24,269	24,269
2	1,72378	21,547	45,817
3	1,25779	15,722	61,539
4	1,06707	13,338	74,877
5	0,708871	8,861	83,738
6	0,592548	7,407	91,145
7	0,455679	5,696	96,841
8	0,252712	3,159	100,000

Table 5. *Factor loadings matrix according to the results of factor analysis after VARIMAX turning*

Quality factors	Factor loadings of quality factors by the numbers of the factor analysis factors			
	1	2	3	4
z1	0,103195	0,380857	-0,705263	0,115358
z2	-0,371948	0,314731	0,249266	-0,692426
z3	0,843849	0,00969395	-0,061031	0,175994
z4	-0,424754	0,817567	-0,0758267	-0,0523348
z5	-0,361204	-0,808773	0,162555	-0,102774
z6	0,775735	0,00757224	0,0223377	-0,284176
z7	0,034402	0,0387176	0,831778	0,136634
z8	0,159447	0,28357	0,279033	0,734205

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

To preserve the condition of comparing the levels of qualitative factors of economic stimulation of top managers' labor in dynamics, it is advisable to calculate the integral indicator according to the data, spatially dynamic with the use of factor loadings (tab. 5). Thus, the first latent factor of economic stimulation of top managers' labor has the form:

$$F_1 = 0,103z_1 - 0,372z_2 + 0,844z_3 - 0,425z_4 - $$
$$-0,361z_5 + 0,776z_6 + 0,034z_7 + 0,159z_{8.}$$

This factor explains 24.269% of the dispersion (variability) of the initial system of qualitative factors, which are the largest contribution to the total cumulative dispersion, so it should be used to determine the integral index. Thus, the formula for the integral index (I) looks as follows:

$$I = 0,1031\bar{z}_1 - 0,3722\bar{z}_2 + 0,8443\bar{z}_3 - 0,4254\bar{z}_4 - $$
$$-0,3615\bar{z}_5 + 0,7766\bar{z}_6 + 0,0347\bar{z}_7 + 0,1598\bar{z}_8.$$

By substituting the average values of the qualitative factors, we obtain the level of the integral qualitative indicator. The scale of this integral indicator is also five-point and corresponds to the levels: very low (1 - very weak), low (2 - weak), sufficient (3 - sufficient), high (4 - significant), very high (5 - very strong)).

Besides this factor, there are three more with the following expression:

$$F_2 = 0,381z_1 + 0,315z_2 + 0,01z_3 + 0,818z_4 - $$
$$- 0,809z_5 + 0,008z_6 + 0,039z_7 + 0,284z_{8,}$$

this factor explains 21.547% of the dispersion of the initial system of quality factors;

$$F_3 = -0,705z_1 + 0,249z_2 - 0,061z_3 - 0,076z_4 + $$
$$+0,163z_5 + 0,022z_6 + 0,832z_7 + 0,279z_{8,}$$

this factor explains 15,722% of the dispersion of the initial system of quality factors;

$$F_4 = 0,115z_1 - 0,692z_2 + 0,176z_3 - 0,052z_4 - $$
$$-0,103z_5 - 0,284z_6 + 0,137z_7 + 0,734z_{8,}$$

this factor explains 13,338% of the dispersion of the initial system of quality factors.

All four latent factors explain 74.877% of the variability of the values of qualitative factors of economic stimulation of the top managers' labor.

Thus, the dynamics of the integral qualitative indicator of economic stimulation of top managers' labor, calculated using the first latent factor, is presented in fig. 2.

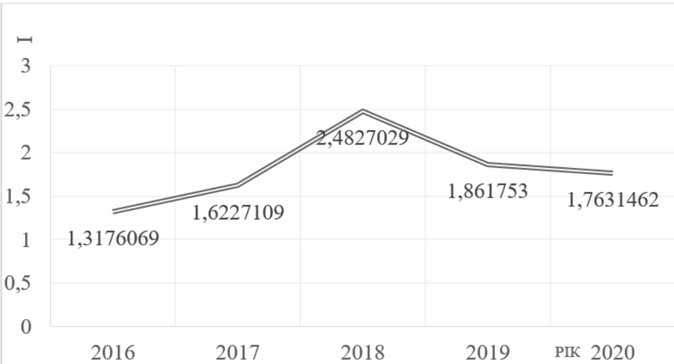


Fig. 2. Dynamics of values of the integral qualitative index of economic stimulation of top managers' labor of the enterprise Private Joint Stock Company "Kharkiv Stamp and Mold Plant"

Consequently, the levels of values of the integral qualitative indicator of economic stimulation of labor of top managers do not exceed the qualitative marks of low (2 - weak), and in the third year - do not exceed sufficient (3 - sufficient). In the last two years, there has been a drop in the level of economic incentives for the work of top managers. This company should urgently develop and disseminate measures to activate the positive effect of the main factors of economic stimulation of top managers' labor.

The given content and the logic of methodological support for determining the level of qualitative economic incentives for top managers' labor were used for the study of 7 enterprises in the Kharkiv region. The dynamics of the qualitative integral index of economic incentives for the work of top managers in 7 enterprises of Kharkiv region is presented in table 6.

Table 6. *Integral quality indicator of economic stimulation of the top managers' labor at the enterprises of the Kharkiv region*

Name of Company	Year				
	1	2	3	4	5
PJSC "Kharkiv Stamp and Mold Plant"	1,318	1,623	2,483	1,862	1,763
TSPC "NOVA"	1,578	1,490	1,670	0,943	2,125
PSPE "Ukrpolitechservice"	0,769	0,455	1,658	0,075	0,684
PE "Promsintez"	1,601	1,698	0,853	1,478	1,041
PJSC "Machine-Building Plant named after Frunze »	1,942	2,956	2,330	2,438	2,093
Khartron Express LTD Research and Production Enterprise (LLC)	0,443	1,368	0,576	0,291	0,008
PJSC Kharkiv Electrotechnical Plant Ukrelectromash	0,811	0,750	0,079	0,971	1,861

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

The analysis of the levels of qualitative indicator of economic stimulation of the top managers' labor in the research enterprises of Kharkiv region has proved the presence of low (weak) level of economic stimulation. Special attention should be paid to the influence of the level of remuneration on the increase of economic stimulation of labor, top managers are not satisfied with the existing system of economic stimulation at the enterprise, and they are not satisfied with the level of wages and the main economic stimulating factor of labor used at the enterprises. In addition, the factor of current material rewards is weak, which also does not affect the amount of monetary rewards received for the results of top managers' work.

Thus, the conducted research has proved that in order to develop methodological support for determining the priority qualitative factors of economic stimulation of top managers' labor it is necessary to justify a questionnaire that characterizes and takes into account the main factors of economic stimulation of top managers' labor and their scales, a set of analytical tools for conducting the analysis. factors, namely, tools of descriptive statistics of order attributes, development of an integral qualitative indicator Such basic aspects of methodological support will allow us to carry out a thorough analysis of qualitative factors of economic stimulation of top managers' labor and determine their level of development at an enterprise in dynamics.

Conclusions

Summarizing, we can conclude that the proposed and substantiated methodological support for determining the priority qualitative factors of economic stimulation of top managers' labor differs from the existing ones: 1) the content of qualitative factors; 2) the analysis of the structure of the studied set of ordering of experts' answers with the help of descriptive statistics tools; 3) the evaluation of the closeness of interrelation of qualitative factors of economic stimulation of top managers' labor in dynamics; 4) the evaluation of consistency of experts' answers in dynamics; 5) identification of latent factors of economic stimulation of top managers' labor; 6) the analytical way of developing the integral qualitative indicator of economic stimulation of top managers' labor.

The main stages, tools and results of the developed methodological support are presented in table 7.

Table 7. *The main stages, methods and results of methodological support for the identification of priority quality factors to stimulate the work of top managers at industrial enterprises*

Content of the methodological support stage	Calculation methods	Result
Rationale of the questionnaire questions that characterize the main qualitative factors of economic stimulation of top managers' labor and their scales	Theoretical generalization and theoretical-logical analysis	Questionnaire to determine the main qualitative factors of economic incentives for the work of top managers
Analysis of the structure of experts' answers to the questionnaire	Descriptive statistics tools	Structure of the studied set of ordering of experts' answers
Assessment of the relationship between the qualitative factors of economic stimulation of top managers' labor in dynamics	Spearman's rank correlation coefficient	Structure of the relationship between qualitative factors of economic stimulation of top managers' labor in dynamics
Evaluation of the consistency of experts' answers in dynamics	Coefficient of concordance	Structure of consistency of experts' answers in dynamics
Revealing the latent factors of economic stimulation of top managers' labor	Factor analysis	Latent factors of economic incentives for top managers' work
Development of the integral qualitative indicator of economic stimulation of top managers' labor	Factor analysis, mean values of factors, additive convolution method	Integral qualitative indicator of economic stimulation of top managers' labor

The practical significance of the developed methodological support is the scientific substantiation, objective determination of real priority qualitative factors, which will allow to form reasonable measures for economic stimulation of the top managers' labor at industrial enterprises.

References

1. Gamova, O. V.(2010), "Salary as an economic category" ["Zarobitna plata yak ekonomichna kategoriya"], *State and Regions: series: Economics and Entrepreneurship*, No. 3, P. 368.
2. Matrosov, O. D., Mykhailyk, S.V. (2013), "Moral and material stimulation of labor" ["Moral'ne ta material'ne stimulyuvannya praci"], *Visnyk Nats. tech. HPI University: Coll. Science. etc. Topic. issue : Technical progress and production efficiency*, No. 22 (995), P. 110–113.
3. Darchenko, N. D., Gitis, T. P. (2013), *Motivation of personnel* [*Motivaciya personala*], textbook , Kramatorsk, DGMA, 139 p.
4. Leshchenko, L. O. (2016), "Motivation of labor as a factor in increasing the profitability of production" ["Motivaciya praci yak faktor pidvishchennya pributkovosti virobnictva"], *Effective Economy*, No. 4.
5. Saati, T. (1993), *Decision making. Hierarchy analysis method* [*Motivaciya praci yak faktor pidvishchennya pributkovosti virobnictva*], Moscow, Radio and communication, 320 p.
6. Malyarets, L. M. (2006), *Measurement of signs of objects in the economy: methodology and practice* [*Vimiryuvannya oznak ob"ektiv v ekonomici: metodologiya ta praktika*], Kharkiv, KhNEU, 384 p.
7. Yeliseyeva, O. K, Kutova, N. G. (2017), "Stimulation in the personnel management system of enterprises" ["Stimulyuvannya v sistemi upravlinnya personalom pidpriemstv"], *Business Inform*, No. 4, P. 388–392.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

8. Kondratenko, N. O, Volkova, M. V, Mahomedova, M. A. (2019), "Foreign Experience of Using the Organization's Motivation and Incentive System", *Business Inform*, No. 12, P. 414–420. DOI: https://doi.org/10.32983/2222-4459-2019-12-414-420
9. Lukyanenko, D., Mozgovyi, O., Burmaka, M. (2015), "Motivation of top management of global corporations" ["Motivaciya top-menedzhmentu global'nih korporacij"], *International economic policy*, No. 2 (23), P. 5–28.
10. Grigorieva, L. (2011), "Development of views on the role and value of top managers" ["Rozvitok poglyadiv na rol' ta cinnist' top-menedzheriv"], *Socio-economic problems and the state*, Issue. 2 (5).
11. Klymchuk, A. O., Mikhailov, A. N. (2018), "The motivation and stimulation of personnel in effective enterprise management and innovation activity improving", *Marketing and Management of Innovations*, No.1, P. 218–234. DOI: http://doi.org/10.21272/mmi.2018.1-16.
12. Karpenko, V. L. (2011), "Directionsof stimulation of top management on assistance to achievement of competitive advantages of the enterprise in the market" ["Napryami stimulyuvannya top-menedzhmentu shchodo spriyannya dosyagnennyu konkurentnih perevag pidpriemstva na rinku"], *Bulletin of Khmelnytsky National University. Ser .: Economic Sciences*, No. 2, Vol. 1, P. 29–34.
13. Ponomarenko, V. S, Malyarets, L. M. (2009), *Data analysis in studies of socio-economic systems*, monograph, "INZHEK", 432 p.
Johan Graafland & Niels Noorderhaven (2020), "Technological Competition, Innovation Motive and Corporate Social Responsibility: 14. Evidence from Top Managers of European SMEs," *De Economist*, Vol. 168 (1), P. 1–22. DOI: https://doi.org/10.1007/s10645-019-09351-z
12. Muhammad, Fiaz & Qin Su & Ikram Amir & Aruba Saqib (2017), "Leadership styles and employees' motivation: Perspective from an emerging economy," *Journal of Developing Areas*, Vol. 51 (4), P. 143–156.
16. Philip, T., Roundy & Ye Dai & Mark A., Bayer & Gukdo Byun (2016), "Motivated to change? TMT regulatory focus and strategic change," *Management Research Review*, Vol. 39 (7), P. 803–829.
17. Momot, T., Filonych, O., Kosiak, A. Lobach, O. (2021), "Balanced scorecard of safety-oriented management for the construction industry enterprises", *Innovative technologies and scientific solutions for industries*, No. 2, P. 54 – 62. DOI: https://doi.org/10.30837/ITSSI.2021.16.054

Received 23.05.2022

Відомості про авторів / Сведения об авторах / About the Authors

Малярець Людмила Михайлівна – доктор економічних наук, професор, завідувач кафедри вищої математики і ЕММ Харківського національного економічного університету імені Семена Кузнеця, Харків, Україна; malyarets@ukr.net; ORCID: https://orcid.org/0000-0002-1684-9805

Малярец Людмила Михайловна – доктор экономических наук, профессор, заведующая кафедрой высшей математики и экономико-математических методов Харьковского национального экономического университета имени Семена Кузнеца, Харьков, Украина.

Malyarets Lyudmula – Doctor of Science (Economics), Professor, Head of the Department of Higher Mathematics, Economic and Mathematical Methods, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine.

Ястремська Олена Миколаївна – доктор економічних наук, професор, завідувач кафедри менеджменту, логістики та інновацій Харківського національного економічного університету імені Семена Кузнеця, Харків, Україна; email: iastremska_om@hneu.net; ORCID: https://orcid.org/0000-0002-5653-6301

Ястремская Елена Николаевна – доктор экономических наук, профессор, заведующая кафедрой менеджмента, логистики и инноваций Харьковского национального экономического университета имени Семена Кузнеца, Харьков, Украина.

Iastremska Olena – Doctor of Science (Economics), Professor, Head of the Department of Management, logistics and Economics of Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine.

Тутова Анастасія Сергіївна – аспірантка кафедри менеджменту, логістики та інновацій Харківського національного економічного університету імені Семені Кузнеця, м. Харків, Україна, email: tutova2605@gmail.com; ORCID: https://orcid.org/0000-0002-8264-9887

Тутова Анастасия Сергеевна – аспирантка кафедры менеджмента, логистики и инноваций Харьковского национального экономического университета имени Семена Кузнеца, Харьков, Украина.

Tutova Anastasiia – Postgraduate student of the Department of Management, Logistics and Innovation Simon Kuznets Kharkiv National University of EconomicsKharkiv, Ukraine

ВИЗНАЧЕННЯ ПРІОРИТЕТНИХ ЯКІСНИХ ФАКТОРІВ СТИМУЛЮВАННЯ ПРАЦІ ТОП-МЕНЕДЖЕРІВ ПІДПРИЄМСТВ

Стаття присвячена обґрунтуванню основних суб'єктивних якісних факторів, які є типовими для стимулювання праці менеджерів стратегічного рівня управління підприємств, і які доцільно враховувати в процесі розроблення системи економічного стимулювання їх діяльності, оскільки базування і визначення обсягів заохочень тільки на статистичній об'єктивній інформації не в змозі суттєво впливати на кінцеві результати діяльності праці топ-менеджерів. **Метою** статті є виявлення пріоритетних якісних факторів впливу на процес економічного стимулювання діяльності топ-менеджерів промислових підприємств та їх кількісна інтерпретація на основі об'єднання якісних оцінок в інтегральний показник. **Завданнями** статті є аналізування результатів анкетування топ-менеджерів щодо окремих якісних факторів впливу на їх умотивованість, визначення статистичного зв'язку між факторами, визначення явних і латентних тенденцій динаміки цих факторів, розрахування інтегрального показника впливу виявлених значущих факторів, формування методичного забезпечення виявлення пріоритетних якісних факторів економічного стимулювання результатів роботи топ-менеджерів промислових підприємств. **Об'єктом** статті є процес економічного стимулювання результатів діяльності топ-менеджерів промислових підприємств. **Предметом** статті є теоретичні положення, методичне забезпечення, практичні пропозиції щодо

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2524-2296 (online)*

економічного стимулювання діяльності менеджерів стратегічного рівня управління промислових підприємств. **Методи.** Для досягнення мети у статті використані такі основні загальні та спеціальні методи дослідження: теоретичне узагальнення, анкетування, інструменти описової статистики, ранговий коефіцієнт кореляції Спірмена, багатовимірний факторний аналіз, метод розрахунку інтегрального показника якісних факторів стимулювання праці менеджерів, графічний метод. **Результати.** В якості результатів дослідження: проаналізовано наукові досягнення попередників щодо формування і використання показників результатів діяльності підприємств як індикаторів стимулювання праці топ-менеджерів; опитувано топ-менеджерів промислових підприємств щодо їх думок про основні фактори впливу на результативність власної діяльності; доведено взаємозв'язок факторів впливу на стимулювання праці топ менеджерів, що представлені в анкеті; виявлено явні та латентні тенденції взаємозв'язку факторів впливу на результативність праці менеджерів стратегічного рівня підприємств; визначено інтегральний показник якісних факторів стимулювання праці менеджерів, кількісні значення якого довели наявність недостатнього врахування факторів на процес стимулювання. **Висновки.** В результаті визначення взаємозв'язку між якісними факторами впливу на економічне стимулювання праці топ-менеджерів розроблено методичне забезпечення, що відрізняється: змістом якісних факторів; аналізом структури досліджуваної сукупності упорядкувань відповідей експертів за допомогою інструментів описової статистики; оцінкою тісноти взаємозв'язку якісних факторів економічного стимулювання праці топ-менеджерів в динаміці; оцінкою узгодженості відповідей експертів в динаміці; виявленням латентних факторів економічного стимулювання праці топ-менеджерів; аналітичним методом розроблення інтегрального якісного показника економічного стимулювання праці топ-менеджерів.

Ключові слова: стимулювання праці; топ-менеджер; промислове підприємство; якісні фактори; взаємозв'язок між якісними факторами; методичне забезпечення.

ОПРЕДЕЛЕНИЕ ПРИОРИТЕТНЫХ КАЧЕСТВЕННЫХ ФАКТОРОВ СТИМУЛИРОВАНИЯ ТРУДА ТОП-МЕНЕДЖЕРОВ ПРЕДПРИЯТИЙ

Статья посвящена обоснованию основных субъективных качественных факторов, типичных для стимулирования труда менеджеров стратегического уровня управления предприятий, и которые целесообразно учитывать в процессе разработки системы экономического стимулирования их деятельности, поскольку базирование и определение объемов поощрений только на статистической объективной информации не способно оказывать существенное влияние на конечные результаты деятельности труда топ-менеджеров. **Целью** статьи является выявление приоритетных качественных факторов влияния на процесс экономического стимулирования деятельности топ-менеджеров промышленных предприятий и их количественная интерпретация на основе объединения качественных оценок в интегральный показатель. **Задачами** статьи являются анализ результатов анкетирования топ-менеджеров относительно отдельных качественных факторов влияния на их мотивированность, определение статистической связи между факторами, определение явных и латентных тенденций динамики этих факторов, расчет интегрального показателя влияния выявленных значимых факторов, формирование методического обеспечения выявления приоритетных качественных факторов экономического стимулирования результатов работы топ-менеджеров промышленных предприятий **Объектом** статьи является процесс экономического стимулирования результатов деятельности топ-менеджеров промышленных предприятий. **Предметом** статьи являются теоретические положения, методическое обеспечение, практические предложения по экономическому стимулированию деятельности менеджеров стратегического уровня управления промышленных предприятий**. Методы**. Для достижения цели в статье использованы следующие основные общие и специальные методы исследования: теоретическое обобщение, анкетирование, инструменты описательной статистики, ранговый коэффициент корреляции Спирмена, многомерный факторный анализ, метод расчета интегрального показателя качественных факторов стимулирования труда менеджеров, графический метод. **Результаты.** В качестве результатов исследования: проанализированы научные достижения предшественников по формированию и использованию показателей результатов деятельности предприятий как индикаторов стимулирования труда топ-менеджеров; опрошены топ-менеджеры промышленных предприятий для выявления их мнений об основных факторах влияния на результативность своей деятельности; доказана взаимосвязь факторов влияния на стимулирование труда топ-менеджеров; выявлены явные и латентные тенденции взаимосвязи факторов влияния на результативность труда менеджеров стратегического уровня предприятий; определен интегральный показатель качественных факторов стимулирования труда менеджеров, количественные значения которого доказали наличие недостаточного учета факторов на процесс стимулирования. **Выводы.** В результате определения взаимосвязи между качественными факторами влияния на экономическое стимулирование труда топ-менеджеров разработано методическое обеспечение, отличающееся: содержанием качественных факторов; анализом структуры изученной совокупности упорядоченых ответов экспертов с помощью инструментов описательной статистики; оценкой тесноты взаимосвязи качественных факторов экономического стимулирования труда топ-менеджеров в динамике; оценкой согласованности ответов экспертов в динамике; выявлением латентных факторов экономического стимулирования труда топ-менеджеров; аналитическим способом разработки интегрального качественного показателя экономического стимулирования труда топ-менеджеров.

Ключевые слова: стимулирование труда; топ-менеджер; промышленное предприятие; качественные факторы; взаимосвязь между качественными факторами; методическое обеспечение.

Бібліографічні описи / Bibliographic descriptions

Малярець Л. М., Ястремська О. М., Тутова А. С. Визначення пріоритетних якісних факторів стимулювання праці топ-менеджерів підприємств. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 75–85. DOI: https://doi.org/10.30837/ITSSI.2022.20.075

Malyarets, L., Iastremska, O. Tutova, A. (2022), "Determination of priority qualitative factors of stimulation of the work of enterprise top managers", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 75–85. DOI: https://doi.org/10.30837/ITSSI.2022.20.075

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 621.865.8 DOI: https://doi.org/10.30837/ITSSI.2022.20.086

I. NEVLYUDOV, S. NOVOSELOV, O. SYCHOVA

DEVELOPMENT AND STUDY OF THE OPERATION OF THE MODULE FOR DETERMINING THE ORIENTATION OF THE MANIPULATOR JOINT

In the field of mechatronic systems, manipulators are often used for automated assembly of products, welding, painting parts and more. An important task is to optimize the travel time along a given trajectory of the manipulator. To solve this problem, it is necessary not only to accurately estimate the speed of the manipulator nodes, but also to provide a linear characteristic of the assessment of the position of the mechanism in a wide range of speeds. The matter of the article are methods for determining the orientation of the joint of the manipulator. The **goal** of the work is to develop a module for determining the orientation of the joint of the manipulator and study its operation in order to determine the suitability **subject** of the structure for practical use. The following **tasks** are solved in the article: to investigate the principles of determining the orientation of the joints of industrial robots; choose the design of the orientation determination module; develop an algorithm for determining the position of the joint at any time; perform experimental studies of the position determination module in order to confirm the suitability of the structure for practical use. The following **methods** used are: experimental research was conducted on a real object - a model of the manipulator joint, created using methods and tools of 3D prototyping; to determine the position of the joint of the manipulator used methods of processing signals received from sensors; processing of experimental results and calculation of values of errors of positioning of a joint of the manipulator is based on methods of the statistical analysis of random sizes. The following **results** were obtained: the principles of determining the orientation of the joints of industrial robots were studied; the design is developed and the module of definition of orientation of a joint of the manipulator is created; developed an algorithm for determining the position of the joint at any time; the suitability of the design for practical use has been experimentally confirmed. **Conclusions:** in this paper, two variants of the sensor design are proposed to determine the absolute angle of rotation of the manipulator joint: resistive and magnetic. The proposed design of the resistive sensor was non-technological and much larger than the design of the magnetic sensor. The data obtained in the process of conducting experimental studies of the proposed method of measuring the angle of rotation of the mechanical gearbox of the manipulator joint indicate a fairly accurate determination of the angle using a magnetic sensor. The calculated measurement error was less than 1.4 degrees. The results of the experiment also showed that in addition to the radial direction of movement of the gearbox of the manipulator joint there is a significant displacement along the working plane, and in some cases, such displacements are chaotic. This is due to some defects and imperfections of the surface of the manufactured parts of the joint model used in research.

Keywords: manipulator; positioning; orientation; angular rotation; designing; industrial robot.

Introduction

Manipulator robots are devices most commonly used in mechatronic systems for automated product assembly, welding, painting parts, etc. The main task of a manipulator is to place the working elements at a given point in space. Most often, this task is solved by using position sensors and adjustable drives. A separate requirement for the operation of technological units is to optimize the movement time by a given trajectory. To solve this problem, it is necessary not only to accurately estimate the speed of movement of manipulator units, but also to provide a given characteristic of estimating the position of the mechanism in a wide range of velocity changes. Thus, the study of methods for determining the position of structural elements at any point of time is quite an urgent task.

Analysis of recent studies and publications

In [1], the authors proposed a methodology for obtaining a sequential chain with less than five connections to realize an approximate end-effector trajectory as close to the target trajectory as possible without selecting any specific positions. This approach is useful when it is difficult to select certain important positions along the target trajectory or when a smooth motion trajectory is required to move along the target trajectory.

Considering the dynamics of the system at [2], the authors proposed a flexible computational approach to optimize the design of robots with open and closed-loop trajectory of motion, using the implicit function theorem. The research of the problem considered in this paper focuses mainly on kinematic synthesis for the implementation of a sequential manipulator circuit, which can help to achieve given configurations of the final effect.

In [3], a method is proposed to optimize the trajectories of robotic arms having manipulators with six degrees of freedom (DOF) and spherical wrists. The trajectories are optimized by maximizing manipulator performance (manipulability). For this purpose, the authors have defined kinematic models of the robot arms, which can be integrated into the algorithm based on the Kalman filter

An adaptive controller based on a nonlinear sliding mode scheme is presented in [4] to control the position of the robot manipulator. The impact of system nonlinearity, uncertainty and unpredictable perturbations is compensated by model-free estimation. The control assignment is implemented using a two-layer control signal. An adaptation capability is built in at the level of the control architecture.

The determination of the position parameters of the joint parts [5] is based on independent measurements using dual encoders mounted on the drive motor and the drive joint. In addition, in [6] it is proposed to calibrate manipulator positions by QR code.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

Allocating the previously unsolved parts of the general problem. The aim of the work

To solve the problem of optimization of movement time along a given manipulator trajectory, it is necessary not only to accurately estimate the speed of manipulator nodes, but also to provide a linear characteristic of estimating the position of the mechanism in a wide range of speed changes. It is also important to determine the absolute angular position of manipulator design elements, especially in the interaction of industrial automation objects using the Internet of Things technology [7-11]. Thus, the study of methods for determining the position of structural elements of the manipulator at any point in time is an urgent task. The **subject** of this research are methods for determining the orientation of the manipulator joint. The **aim** of the work is to develop a module for determining the orientation of the manipulator joint and study its operation in order to determine the suitability of the design for practical use.

In order to achieve the set objectives, it is necessary to solve the following tasks:

- to investigate the principles of joint orientation determination of industrial robots;
- to select the design of the orientation determination module;
- to develop an algorithm for determining the joint position at any time;
- to carry out an experimental study of the operation of the position determination module in order to confirm the suitability of the design for practical use.

Materials and methods

Manipulator motion control by individual movement steps can be continuous (contour) or discrete (positional). With discrete control, motion control is performed by specifying a finite sequence of points and then moving through them in steps from point to point. The simplest type of discrete control is cyclic control, in which the number of positioning points for each degree of mobility is minimal and usually limited to two - the initial and final coordinates. The most important parameters of manipulators are speed and accuracy of movements. These parameters are interrelated and characterize the dynamic characteristics of robots. The speed of a manipulator is determined by the speed of its movement through the individual degrees of mobility. Most modern robots have an average speed and only 20% have a high speed. The speed of modern robots is still insufficient, and it is necessary to increase it at least twice. The main difficulties here are related to the well-known contradiction between speed and accuracy. The accuracy of a manipulator is characterized by the resulting positioning error (in discrete motion), or by the execution of a given trajectory (in continuous motion). More often, the accuracy of robots is characterized by the absolute error. The accuracy of robots of general application is divided into three groups:

- small – with a linear error of 1 mm or more;
- medium – with linear error from 0,1 to 1 mm;
- high – with a linear error of less than 0.1 mm.

In this case, the speed of linear movement of the working elements of manipulators does not exceed 1 m/s, although there are some jobs with speeds up to 2 m/s and more. Angular speeds of movements of working elements are mainly in the range of 15...360 deg. /sec.

To determine the position of the manipulator joint, we used methods for processing the signals received from the sensors. Experimental results processing and calculation of positioning error values of the manipulator joint are based on the methods of statistical analysis of random variables. Experimental studies were performed on a real object - a model of a robotic manipulator joint, created using the methods and means of 3D prototyping.

Analysis and development of the design of the manipulator joint model

A special model - a robotic manipulator joint - was made for the research. Fig. 1 shows its appearance.

Fig. 1. Appearance of the robot-manipulator joint

The design of the joint should include the principle of fixing a sensor to determine the position of the mechanism when the device is in operation. Figure 2 shows a sketch of the moving part of the manipulator design.

The base of the manipulator model is rigidly fixed on the working surface. A first stepper engine is built into the base. A movable attachment is mounted on the motor shaft. The lower arm structure of the manipulator is mounted on it. Activation of the motor leads to the action of the planetary gear mechanism. Due to it the upper part

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

of the structure is set in motion relative to the lower part, as shown in fig. 2, b (dashed arrow).

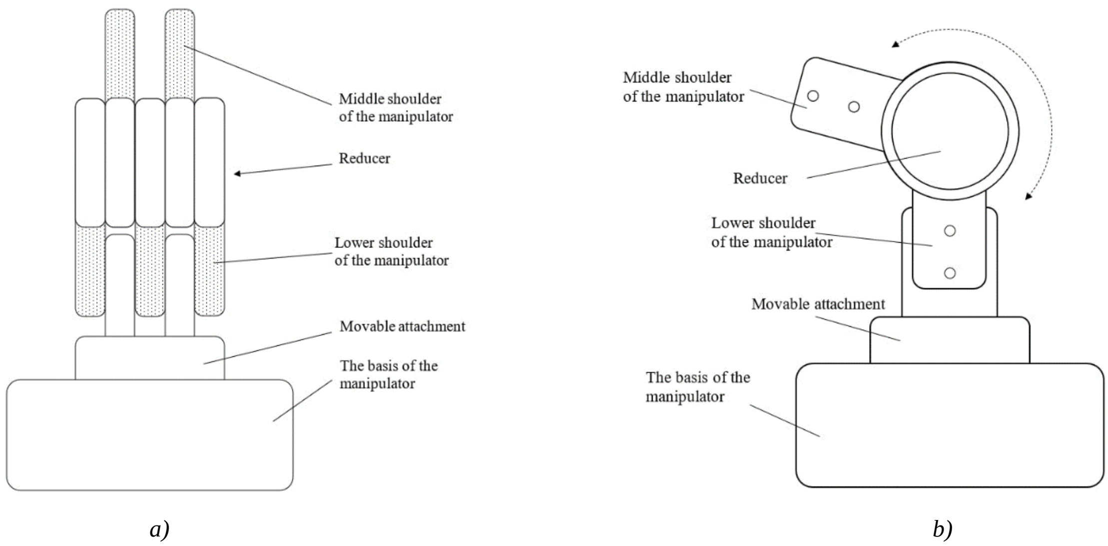


Fig. 2. Drawing of the moving part of the manipulator structure: a - front view; b - side view

There are four sections in the reducer design. Two rotate clockwise and two rotate counterclockwise. Fig. 3 shows how the reducer works. As you can see from this figure, the two sections of the reducer always rotate synchronously and in the same direction. For the application of the reducer, the design of the arm of the manipulator was developed. The reducer is inserted into the arm hole and secured with pins and glue. Four of these parts are needed for one arm. To reduce the number of part sizes, one standard solution was used for the entire arm design.

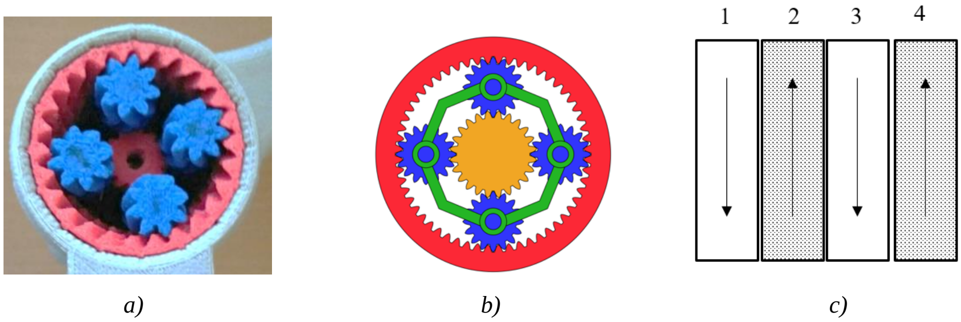


Fig. 3. Principle of operation of the reducer: *a* – reducer inserted into the opening of the section arm; *b* – drawing of the reducer; *c* – direction of rotation of the reducer sections

The main parts of the planetary gears are: the central gear wheel, which is stationary, the satellites - gears with movable rotation axes, and the driver - the link in which the satellites' axes are mounted. As a rule, planetary mechanisms are made coaxial.

Fig. 4, a shows a view of the assembled joint of the manipulator with a mounted gearbox, and fig. 4, b - the principle of fixing the stepper motor to the reducer. The motor axle is tightly inserted into the drive wheel due to the properties of ABS material to transfer the motion without skipping.

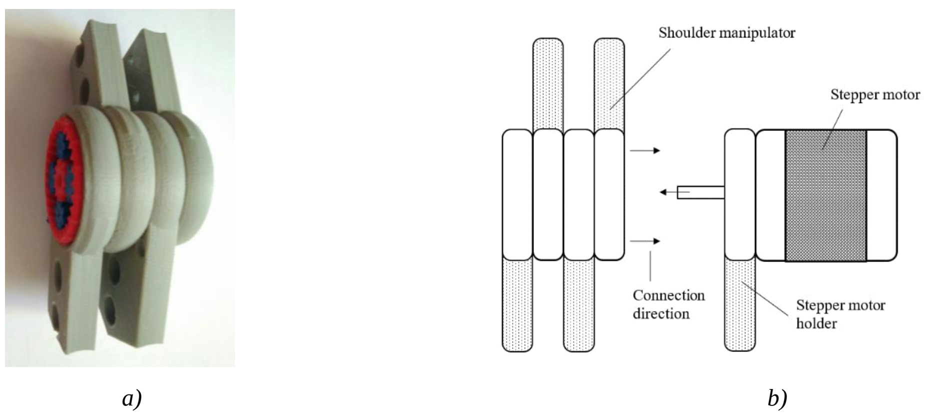


Fig. 4. Manipulator joint assembled with reducer (a); principle of stepper motor attachment to the reducer (b)

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

The result of the joint test was positive - the reducer transmitted motion to the other arm of the manipulator. The study of the design of the manipulator joint model and the analysis of the principles of operation of the driving reducer of its joint showed that the planetary reducer reduces the total number of motor revolutions by 40 times. Using traditional encoders to determine the angular position without using a special mount design is impossible. For further research, it was decided to use two types of encoders: absolute resistive multiturn and absolute magnetic, designed for only one revolution. As a result of further research, the more accurate and technologically advanced version will be chosen.

Development of a test bench design

The structural scheme of the developed test bench is shown in fig. 5.

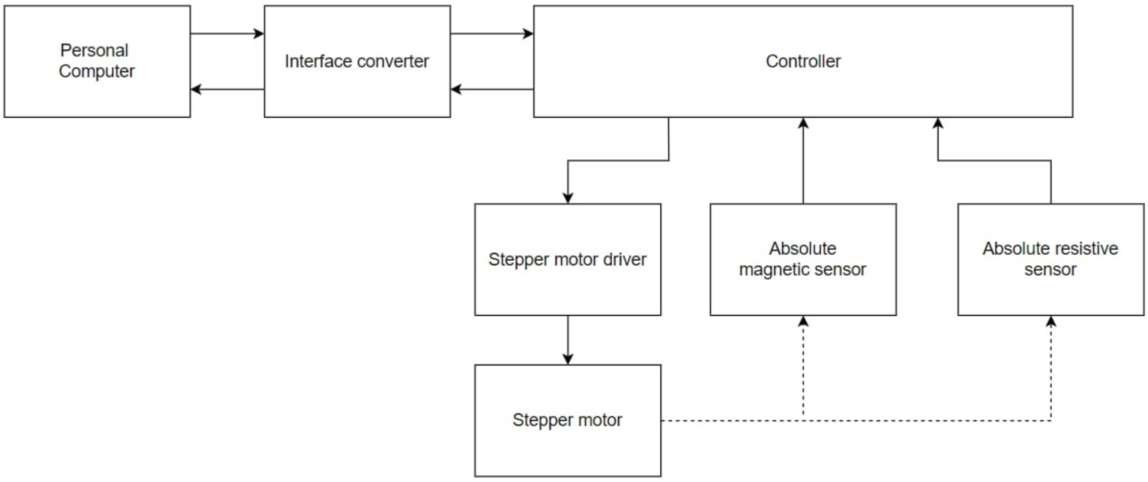


Fig. 5. The structural scheme of the model

The bench consists of the following elements:

- personal computer (PC) with control and data acquisition program;
- interface converter;
- controller;
- DC motor driver;
- absolute magnetic sensor;
- absolute resistive sensor;
- stepper motor;
- model of the manipulator mechanism.

We will use two methods to determine the joint orientation:

- magnetic absolute;
- resistive absolute.

Magnetic sensor design

To determine the absolute angle of rotation of the joint we will use a magnetic encoder type AS5600. This encoder needs an additional element - a magnet, which will be attached to the structural elements of the joint on the same axis as the reducer.

Due to the design of the planetary reducer, the permanent magnet cannot be attached directly to the reducer axis. First, this is due to the fact that the central element of the reducer is the central gear wheel, which makes significantly more revolutions than the manipulator joint. As a result, it was decided to make an additional attachment to the joint, which would be rigidly connected to it and fix a permanent magnet already to it. A drawing of the magnet mount design is shown in fig. 6, a.

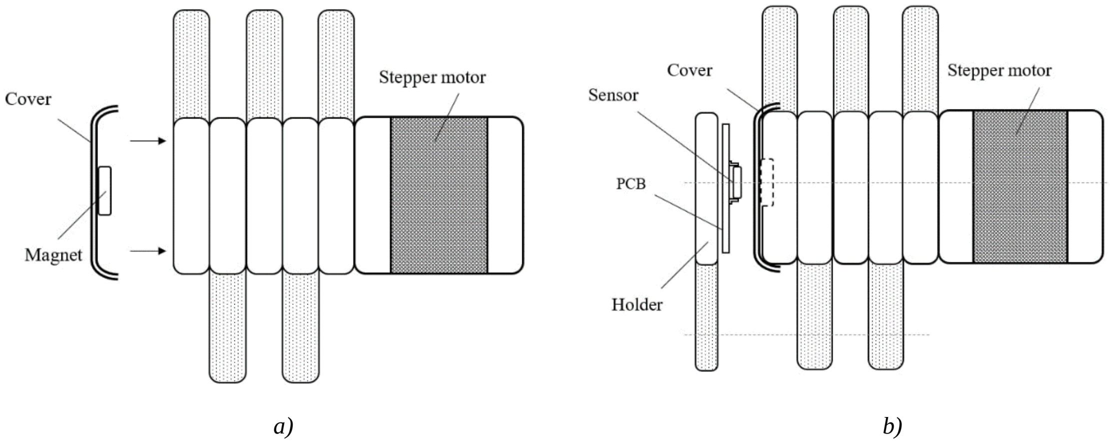


Fig. 6. Principle of attachment of the magnet to the manipulator joint (a); drawing of the reading module attachment variant (b)

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

The cover has to adapt to the parameters of the joint reducer holder due to its design. The design of the reducer used in the model has a peculiarity - the free space between the satellites within the fourth section of the reducer due to the shortened length of the central pinion (fig. 3, a). Thus, there is an opportunity to place the magnet in the empty space of the reducer, which makes the cover design more flat.

In order to determine the angular position of the joint, another design element must be added - the position reading module and its holder. The reading module is based on the AS5600 chip and is a printed circuit board with the required attachments. The printed circuit board is attached to the bracket, which in turn is attached to the base of the layout. Electrical wiring connects the position readout module to the controller to convert the analog signal into digital combinations, process and transmit to a personal computer for analysis. Fig. 6, b shows a drawing of a mounting option for the readout module.

The AS5600 sensor must be positioned precisely on the axis of the reducer and the permanent magnet, respectively. The distance between the sensor and the permanent magnet should be minimal and not exceed 4 mm. In this design, the sensor is rigidly attached to the moving part of the joint on the base of the model. The maximum rotation angle of the joint is 200 degrees. This limitation is due to the design of the prototype.

Fig. 7 shows a drawing of the prototype. In this figure, you can see that in addition to the manipulator joint model itself there is also a control device, the role of which is performed by a protractor. It is used to visually determine the deflection angle of the manipulator arm.

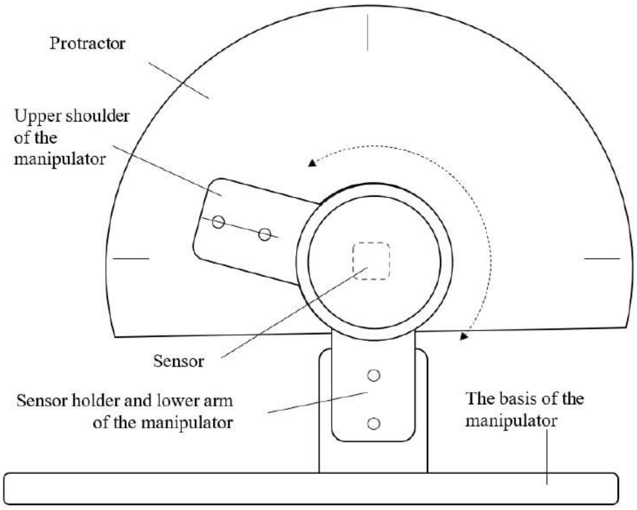
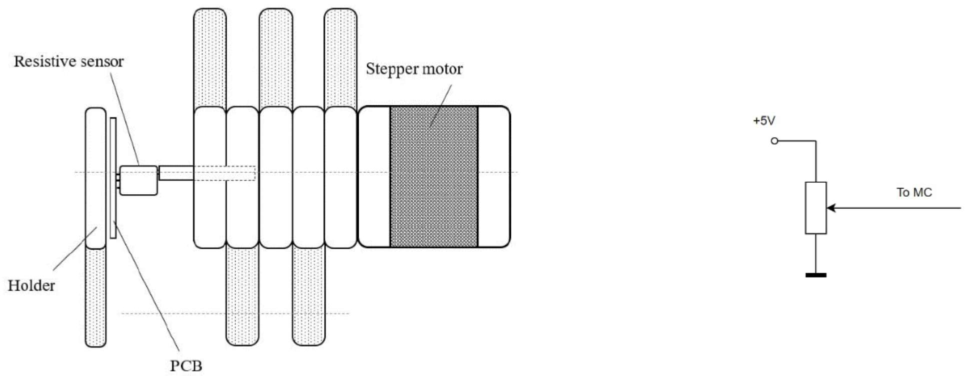


Fig. 7. Drawing of the model

Development of the resistive sensor design

The 3296Y-10K is used as a resistive sensor. This type of resistor is characterized by a large number of revolutions (28 revolutions). Considering the reducer ratio of 1:40, this number of revolutions is enough to shift the arm by 200 degrees. The screw for setting the resistor is quite small. This is a disadvantage in this case, as it adds complexity to the design of the mount and adapter to the reducer.

As mentioned above, the resistor has a large number of revolutions, so it can be connected directly to the central gearwheel with an adapter and determine the angle of rotation based on the current resistor resistance value obtained. It takes 23 revolutions of the central reducer wheel to rotate the arm by 200 degrees. Therefore, this resistor is suitable for the task of determining the absolute angle. Fig. 8, a shows a design of the absolute resistive sensor.



a) b)

Fig. 8. Drawing of the absolute resistive sensor design (a); connection diagram of the resistive sensor to the controller (b)

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

The resistor represents the amount of free space inside the reducer, so the sensor itself must be located at a much greater distance from the reducer than the magnetic sensor. This distance depends on the size of the resistor and is more than 10 mm. This is another disadvantage of this type of sensor design.

The output of the sensor, as in the case of the magnetic sensor, is analog. The sensor is connected to the controller input according to the circuit shown in fig. 8, b. This circuit is a kind of voltage divider and is often used to determine the input voltage in analog circuits for measuring electrical quantities. Thanks to the multi-turn resistor, the accuracy of the joint position measurement is ±4%.

Experimental studies

At the beginning of the experiment, the operator visually checks the position of the arm of the manipulator and moves it to the zero position. The position is determined by means of a protractor. Then the desired angle of rotation is set. The stepper motor control program is started and waits until it finishes its work. Then the controller receives the signal from the AS5600 absolute encoder and sends it to the PC for analysis. At the same time, the operator records the position of the arm using a protractor and enters the values into the corresponding cell in the measurement table. All data from the experiment is recorded for theoretical investigations and positioning error determinations. The current angle of rotation is set from the personal computer and the control signals to the DC motor are applied with the help of the control controller. Fig. 9 shows the algorithm of the model operation.

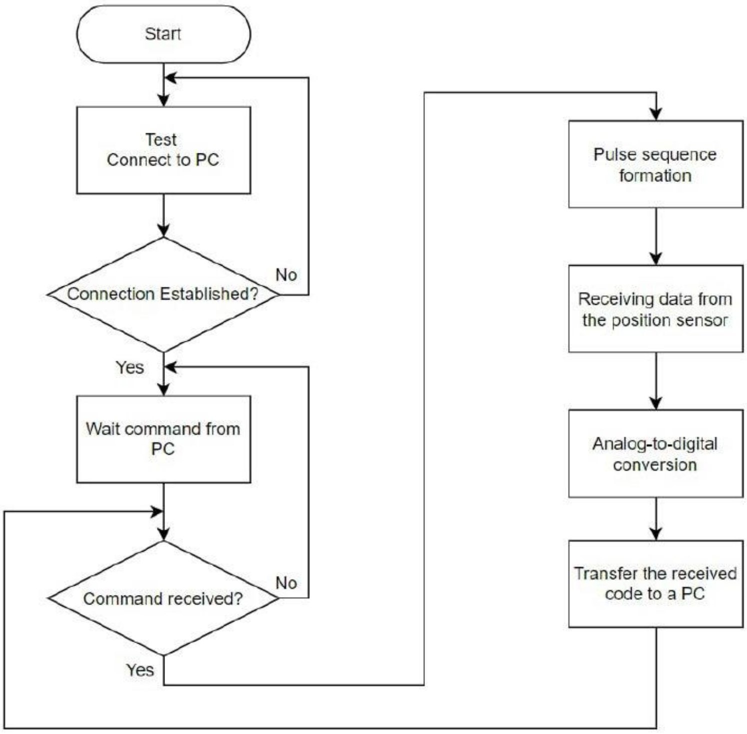


Fig. 9. Controller program algorithm

At the beginning of the work the communication with the personal computer via the serial interface is checked. If the connection is established, you can continue to work. After receiving a command from the PC, the controller forms a sequence of pulses to shift the stepper motor shaft to the desired angle, taking into account the transmission ratio of the reducer. In our case, this number is 1:42. The angle of displacement of the motor shaft at full step is 1.8 degrees. Given the gear ratio, the mechanism can theoretically provide an accuracy of 0.045 degrees.

When the movement is complete, the controller stops the reducer and reads the position sensor data. The data obtained are converted from an analog signal into a digital signal and transmitted to the PC. After the rotation angle measurement is completed, the control cycle is repeated until the controller power supply is turned off. At this stage, the positioning accuracy is determined visually by comparing the values set by the operator and the actual values obtained from the protractor. Figure 10 shows the appearance of the model.

The prototype includes a control module based on Arduino Mega 2560, a reducer model and a measuring device. The protractor is used to visually control the accuracy of the movement. Control lines for measuring the angle of rotation are plotted in 5-degree increments. The center part must be aligned with the center axis of the reducer. To determine the angle more accurately, a pointer arrow is attached to the moving part of the reducer.

An absolute magnetic encoder is used to electrically control the angle of rotation. The encoder board is

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

attached to the reducer with a bracket. The reducer is completely made by 3D printing.

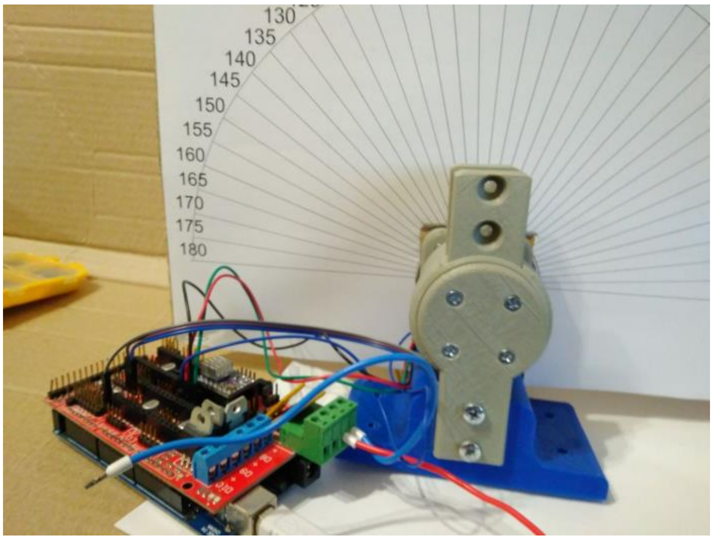


Fig. 10. Appearance of the model

The application written for the Arduino controller was used for the experimental research. The operator has the ability to enter control commands to perform a turn by a certain number of steps or degrees. The command "S" big turns on the counterclockwise rotation mode for 230 steps. The "s" small command enables the clockwise rotation mode for 230 steps. The stepper motor moves 230 steps in one measurement cycle, which is 5 degrees when transferred to the angle of rotation.

To control the driver it is necessary to output one clock pulse for each step. The DIR pin must be set high or low to determine the direction of rotation. After each step, the voltage at the analog output of the absolute position sensor is measured and transmitted through a serial interface to the computer [12, 16]. Table 1 shows the experimental data. The experiment was performed for both clockwise and counterclockwise rotation. This was done to determine the positioning accuracy of the reducer in different directions of operation.

Table 1. *The experiment results*

Measurement number	Expected value of the rotation angle	The value of the position sensor when turning counterclockwise	Measured angle of rotation with a protractor	Position sensor value for clockwise rotation	Measured angle of rotation with a protractor
1	90	124	90	124	90
2	95	133	94	133	96
3	100	148	101	149	103
4	105	163	105	163	108
5	110	180	110	180	114
6	115	196	115	195	118
7	120	196	116	197	120
8	125	217	123	217	125
9	130	229	127	229	129
10	135	251	133	251	135
11	140	260	137	259	140
12	145	278	144	278	146
13	150	289	149	289	150
14	155	300	154	300	155
15	160	320	159	320	159

Fig. 11 shows a graph of the change in the measured parameter. It is possible to observe the anomalous behavior of the graph at the moment of change of rotation angle from 115 to 120 degrees. The measurements showed the absence of radial movement of the reducer. The same behavior was observed during the reverse rotation of the reducer. This was due to a mechanical flaw in the design made by 3D printing.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

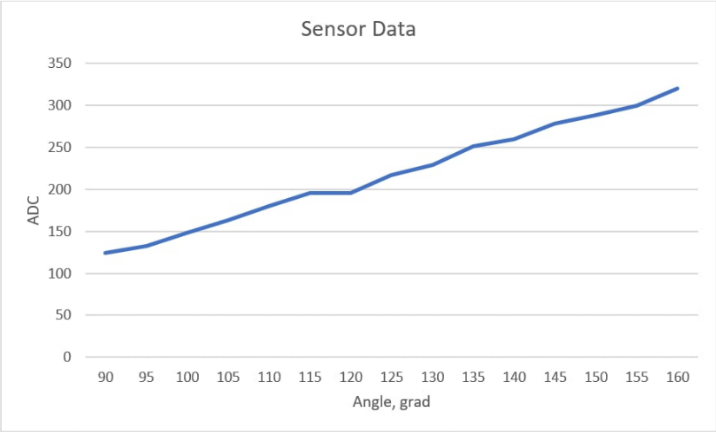


Fig. 11. The graph of change of the measured parameter

Analysis of the results of the experiment. Determination of the magnitude of the error

The positioning error arises due to the error of processing by the drives of the system of programmed values of coordinates corresponding to the given position of the sensor.

During the experiment, the actual values of the sensor coordinates differ from the programmed values by the value Δq_i of where i is a coordinate number. If a Cartesian rectangular coordinate system is linked to the sensor, then the given (programmed) position $X_g Y_g Z_g$ will differ from its actual position $X_a Y_a Z_a$ by the value:

$$\Delta r = \sqrt{\left(X_g - X_a\right)^2 + \left(Y_g - Y_a\right)^2 + \left(Z_g - Z_a\right)} = = \sqrt{\Delta q_1^2 + \Delta q_2^2 + \Delta q_3^2} . \quad (1)$$

The value Δr is called the linear positioning error, and the angle of rotation ϕ by which the system $X_g Y_g Z_g$ must be rotated to make its axes parallel to the corresponding axes of the system $X_a Y_a Z_a$ is called the angular positioning error. Such a rotation is always possible based on the well-known Euler-Dalembert theorem. The radius vector $\overline{r}$ of a random sensor point can be written in the form:

$$\overline{r} = r\left(q_i\right), \quad (2)$$

where $i = 1..n$, n is a number of moving degrees of freedom.

By integrating expression (2) over the coordinates q_i, we obtain the following expression:

$$dr = \sum_{i=1}^{n} \frac{\partial r}{\partial q_i} dq_i . \quad (3)$$

If we replace the differentials in expression (3) with finite increments, we can determine the linear positioning error of the sensor Δr:

$$\Delta r = \sum_{j=1}^{p} \Delta \phi_j \overline{e}_j + \sum_{i=1}^{s} \Delta S_i \overline{e}_i , \quad (4)$$

where $\Delta \phi$ and ΔS are errors in the rotary and translational pairs of the positioning mechanism; p – number of rotating pairs; s – number of translational pairs; $\overline{e}_j$ and $\overline{e}_i$ – orts of rotating and translating pairs in the positioning mechanism.

The angular error of the solid position can be defined by an error matrix, which is a matrix of transition from system $X_д Y_д Z_д$ to system $X_з Y_з Z_з$ by rotation by three Euler angles, which are considered small. Since such a matrix contains the value of three Euler angles, it does not allow to express the angular error by a single value. As a result, it is necessary to find a vector formula to cover the yuto error of the sensor position.

Suppose the linear and yuto errors of the sensor are small. Then, based on the known rule of addition of small rotations of a solid body, we can write down the expression:

$$\Delta \phi = \sum_{i=1}^{s} \Delta q_i = \sum_{j=1}^{p} \Delta q_j \overline{e}_j . \quad (5)$$

The linear positioning error of the sensor is most conveniently determined by formula (4), which does not contain the differentiation operation. In this case, the linear error of the position of the mass sensor center Δr_c is defined as

$$\Delta r_c = \Delta \phi_1 \left(\overline{e}_1 \times \overline{r}_{1c}\right) + \Delta S_1 \overline{e}_1 + \Delta \phi_2 \left(\overline{e}_2 \times \overline{r}_{2c}\right) + \Delta S_2 \overline{e}_2 + ... \quad (6)$$

Assuming that the mass center is on the axis of rotation of the sensor on the manipulator, the linear error module is defined as

$$\Delta r_c = \sqrt{\Delta r_{cx}^2 + \Delta r_{cy}^2 + \Delta r_{cz}^2} , \quad (7)$$

where Δr_{cx}, Δr_{cy}, Δr_{cz} – projections of the linear error vector Δr_c on the Cartesian coordinate system axes.

With a one-sided approach to the set points, the positioning error is determined by the value calculated by the formula:

$$\Delta_{pos.val.} = \overline{Z} - Z_{pr.} \pm 3\sigma_{val.} \quad (8)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

where $\bar{Z}$ is an arithmetic mean value of the actual state of the moving part of the reducer (mathematical expectation), mm; $Z_{pr.}$ – the amount of the programmed movement of the moving part of the reducer; $\sigma_{val.}$ – value of the scatter of values from the arithmetic mean (standard deviation), characterizing the effect of random processes, μm.

$$\bar{Z} = \frac{\sum_{i=1}^{n} Z_i}{n}, \quad (9)$$

where n is the number of measurements of the reducer position (n = 5).

The value of the expected estimate of the positioning error variation is calculated by the formula:

$$S = \sqrt{\frac{\sum_{i=1}^{n} \left(Z_i - \bar{Z}\right)^2}{n-1}}. \quad (10)$$

The value of the greatest probable random dispersion of deviations from the arithmetic mean is taken to be

$$\pm 3\sigma = \pm 3S. \quad (11)$$

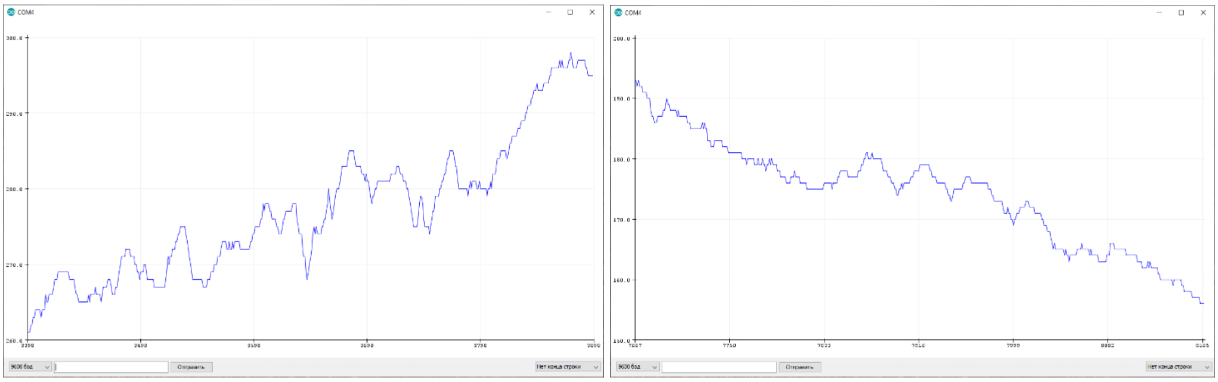
According to the normal law, the dispersion distribution within $\pm 3\sigma$ covers more than 99% of all possible deviations. The results of the estimation of the positioning error are recorded in table 2.

Table 2. *Results of positioning error estimation*

Experiment number	**1**	**2**	**3**	**4**	**5**
Expected angle of rotation	90	110	130	150	160
1 measurement	90	110	127	149	159
2 measurement	90	114	129	150	160
3 measurement	89	114	128	149	160
4 measurement	90	115	124	150	159
5 measurement	90	114	130	149	159
$\bar{Z}$	89,8	113,4	127,6	149,4	159,4
S	0,447213	0,447213	0,447213	0,447213	0,447213
$\pm 3\sigma$	1,341640	1,341640	1,341640	1,341640	1,341640

The data obtained indicate sufficient accuracy of angle determination using a magnetic sensor. The angle measurement error is less than 1.4 degrees. With several consecutive measurements, the displacement of the moving part of the reducer always occurs in the predicted position. However, the results of the experiment also showed poor performance of the reducer itself. In addition to the radial direction of motion, there is a significant displacement along the working plane. The parts undergo considerable displacement, and in some cases, these displacements are chaotic in nature.

Fig. 12 shows the results of continuous measurements for a full rotation angle of the reducer counterclockwise and clockwise. From these figures, you can see how the value of the angle measurement changes depending on the direction of rotation.



a) *б)*

Fig. 12. Results of continuous measurements for a full rotation angle of the reducer: a - counterclockwise rotation; b - clockwise rotation

Conclusions and prospects for further development

In this paper, we proposed two sensor designs for determining the absolute angle of joint rotation: a resistive sensor and a magnetic sensor. The proposed design of the resistive sensor turned out to be non-technological and much larger in size than the design of the magnetic sensor, so it was not used in the research. A model was made using 3D prototyping tools. In this model design, the sensor is rigidly fixed relative to the moving part of the joint on the base of the model. The maximum rotation angle of the joint is 200 degrees. A control device - protractor - is used to visually determine the angle of deviation of the arm of the manipulator.

Experimental studies of the proposed method of measuring the angle of rotation of the mechanical reducer

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) *ISSN 2524-2296 (online)*

of the manipulator joint were conducted. The data obtained show that the angle is accurately determined using a magnetic sensor. The positioning error is less than 1.4 degrees, which is acceptable for reducers of this type, fully manufactured using 3D printing.

However, the results of the experiment also showed the disadvantages of the reducer design related to the manufacturing technology using 3D printing. In addition to the radial direction of motion, there is a significant displacement along the working plane, and in some cases, such displacements are of a chaotic nature. Thus, in the future it is necessary to study the influence of technological printing parameters on the quality of positioning of the manipulator joints.

References

1. Shirafuji, S., Ota, J. (2019), "Kinematic Synthesis of a Serial Robotic Manipulator by Using Generalized Differential Inverse Kinematics", *IEEE Transactions on Robotics*, Vol. 35, No. 4, P. 1047–1054. **DOI:** https://doi.org/10.1109/TRO.2019.2907810.
2. Ha, S., Coros, S., Alspach, A., Kim, J., Yamane, K. (2018), "Computational co-optimization of design parameters and motion trajectories for robotic systems", *Int. J. Robot. Res*, Vol. 37, No. 13–14, P. 1521–1536.
3. Garriz, C., Domingo, R. (2019), "Development of Trajectories Through the Kalman Algorithm and Application to an Industrial Robot in the Automotive Industry", *IEEE Access*, Vol. 7, P. 23570–23578. **DOI:** https://doi.org/10.1109/ACCESS.2019.2899370.
4. Xuan Ba, D., Bae, J. (2020), "A Nonlinear Sliding Mode Controller of Serial Robot Manipulators With Two-Level Gain-Learning Ability", *IEEE Access*, Vol. 8, P. 189224–189235. **DOI:** https://doi.org/10.1109/ACCESS.2020.3032449.
5. Yin, M., Wu, H., Xu, Z., Han, W., Zhao, Z. (2020), "Compliant Control of Single Tendon-Sheath Actuators Applied to a Robotic Manipulator", *IEEE Access*, Vol. 8, P. 37361–37371. **DOI:** https://doi.org/10.1109/ACCESS.2020.2973173.
6. Zhang, Y., Zhu, W., Rosendo, A. (2019), "QR Code-Based Self-Calibration for a Fault-Tolerant Industrial Robot Arm", *IEEE Access*, Vol. 7, P. 73349–73356. **DOI:** https://doi.org/10.1109/ACCESS.2019.2920429.
7. Tantawi, K. H., Sokolov, A., Tantawi, O. (2019), "Advances in Industrial Robotics: From Industry 3.0 Automation to Industry 4.0 Collaboration", *4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*, P. 1–4. **DOI:** https://doi.org/10.1109/TIMES-iCON47539.2019.9024658.
8. Goel, R., Gupta, P. (2019), "Robotics and industry 4.0" in A Roadmap to Industry 4.0", *Smart Production Sharp Business and Sustainable Development*, Cham, Switzerland: Springer, P. 157–169, available at : https://www.springer.com/ gp/book/9783030145439.
9. Shehu, N., Abba, N. (2019), "The role of automation and robotics in buildings for sustainable development", *J. Multidisciplinary Eng. Sci. Technol*, Vol. 6, No. 2, P. 9557–9560.
10. Nevludov, I., Sychova, O., Andrusevich, A., Novoselov, S., Mospan, D., Mospan, V. (2020), "Simulation of the Sensor Network of Base Stations in a Local Positioning System in Intelligent Industries", *IEEE Problems of Automated Electrodrive. Theory and Practice (PAEP)*, Kremenchuk, Ukraine, P. 1–6. **DOI:** https://doi.org/10.1109/PAEP49887.2020.9240842.
11. Lai, R., Lin, W., Wu, Y. (2018), "Review of Research on the Key Technologies Application Fields and Development Trends of Intelligent Robots", *International Conference on Intelligent Robotics and Applications*.
12. Nevlyudov, I. S., Krivoplyas-Volodina, L. O., Novoselov, S. P., Sychova, O. V. (2021), *Electropneumatic automatic drives in automated control systems* [*Elektropnevmoavtomatychni pryvody v avtomatyzovanykh systemakh keruvannia*], textbook. Ministry of Education and Science of Ukraine, Kharkiv, National University of Radio Electronics, Kharkiv, P. 292. **DOI:** https://doi.org/10.30837/978-966-659-332-3.
13. Roveda, L. (2019), "Adaptive Interaction Controller for Compliant Robot Base Applications", *IEEE Access*, Vol. 7, P. 6553–6561. **DOI:** https://doi.org/10.1109/ACCESS.2018.2889849.
14. Nevliudov, I., Novoselov, S., Sychova, O. Tesliuk, S. (2021), "Development of the Architecture of the Base Platform Agricultural Robot for Determining the Trajectory Using the Method of Visual Odometry", *IEEE XVIIth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, Polyana (Zakarpattya), Ukraine, P. 64–68. **DOI:** https://doi.org/10.1109/MEMSTECH53091.2021.9468008.
15. Zhang, S., Wang, S., Jing, F., Tan, M. (2019), "A Sensorless Hand Guiding Scheme Based on Model Identification and Control for Industrial Robot", *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 9, P. 5204–5213. **DOI:** https://doi.org/10.1109/ TII.2019.2900119.
16. Nevlyudov, I. Sh., Novoselov, S. P., Sychova, O. V. (2019), *Technology of industrial controllers programming in an integrated environment CODESYS* [*Tekhnolohiia prohramuvannia promyslovykh kontroleriv v intehrovanomu seredovyshchi CODESYS*], textbook. Ministry of Education and Science of Ukraine, National University of Radio Electronics, Kharkiv, P. 264. **DOI:** https://doi.org/10.30837/978-966-659-265-4.

Received 23.05.2022

Відомості про авторів / Сведения об авторах / About the Authors

Невлюдов Ігор Шакирович – професор, доктор технічних наук, Харківський національний університет радіоелектроніки, завідувач кафедри комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: igor.nevliudov@nure.ua; ORCID ID: https://orcid.org/0000-0002-9837-2309.

Невлюдов Игорь Шакирович – профессор, доктор технических наук, Харьковский национальный университет радиоэлектроники, заведующий кафедрой компьютерно-интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Nevlyudov Igor – Professor, Doctor of Engineering Sciences, Kharkiv National University of Radio Electronics, Head at the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

Новоселов Сергій Павлович – доцент, кандидат технічних наук, Харківський національний університет радіоелектроніки, професор кафедри комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: sergiy.novoselov@nure.ua; ORCID ID: https://orcid.org/0000-0002-3190-0592.

Новоселов Сергей Павлович – доцент, кандидат технических наук, Харьковский национальный университет радиоэлектроники, профессор кафедры компьютерно-интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Novoselov Sergiy – Associate Professor, Candidate of Engineering Sciences, Kharkiv National University of Radio Electronics, Professor at the Department of Computer Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

Сичова Оксана Володимирівна – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: oksana.sychova@nure.ua; ORCID ID: https://orcid.org/0000-0002-0651-557X. Моб. 067-682-21-63.

Сычева Оксана Владимировна – кандидат технических наук, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерно-интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Sychova Oksana – Candidate of Engineering Sciences, Kharkiv National University of Radio Electronics, Associate Professor at the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

РОЗРОБКА МОДУЛЯ ВИЗНАЧЕННЯ ОРІЄНТАЦІЇ СУГЛОБА МАНІПУЛЯТОРА І ДОСЛІДЖЕННЯ ЙОГО РОБОТИ

В галузі мехатронних систем часто використовуються роботи-маніпулятори для автоматизованого збирання виробів, зварювання, фарбування деталей тощо. Важливим завданням при цьому є оптимізація часу руху по заданій траєкторії маніпулятора. Для вирішення такого завдання, необхідно не тільки точно оцінити швидкість руху вузлів маніпулятору, але і забезпечити лінійну характеристику оцінки позиції механізму в широкому діапазоні зміни швидкостей. **Предметом** дослідження в статті є методи визначення орієнтації суглобу маніпулятора. **Мета** роботи – розробка модуля визначення орієнтації суглобу маніпулятору і дослідження його роботи з метою визначення придатності конструкції для практичного використання. В статті вирішуються наступні **завдання:** дослідити принципи визначення орієнтації суглобів промислових роботів; обрати конструкцію модуля визначення орієнтації; розробити алгоритм визначення позиції суглобу в будь-який час; виконати експериментальні дослідження роботи модуля визначення позиції з метою підтвердження придатності конструкції для практичного використання. Використовуються такі **методи:** експериментальні дослідження проводилися на реальному об’єкті – моделі суглобу робота-маніпулятора, створеного за допомогою методів і засобів 3D-прототипування; для визначення положення суглобу маніпулятора використовувалися методи обробки сигналів, отриманих від датчиків; обробка результатів експериментів і розрахунок величин похибок позиціонування суглобу маніпулятора базується на методах статистичного аналізу випадкових величин. Отримано наступні **результати:** досліджено принципи визначення орієнтації суглобів промислових роботів; розроблено конструкцію і створено модуль визначення орієнтації суглобу маніпулятора; розроблено алгоритм визначення позиції суглобу в довільний час; експериментально підтверджено придатність конструкції для практичного використання. **Висновки:** в даній роботі запропоновано два варіанта конструкції датчика для визначення абсолютного куту оберту суглоба маніпулятора: резистивний і магнітний. Запропонована конструкція резистивного датчика виявилася нетехнологічною і набагато більша за розмірами ніж конструкція магнітного датчика. Отримані в процесі проведення експериментальних досліджень запропонованого методу вимірювання куту оберту механічного редуктора суглобу маніпулятора дані свідчать про досить точне визначення кута за допомогою магнітного датчика. Розрахована похибка вимірювань становила менше 1,4 градуси. Також результати експерименту показали, що крім радіального напрямку руху редуктора суглобу маніпулятора відбувається істотне зміщення вздовж робочої площини, причому в деяких випадках такі зміщення мають хаотичний характер. Це обумовлюється деякими дефектами і недосконалістю поверхні виготовлених деталей моделі суглобу, що використовувалися у дослідженнях.

Ключові слова: маніпулятор; позиціонування; орієнтація; кутове обертання; проектування; промисловий робот.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ РАБОТЫ МОДУЛЯ ОПРЕДЕЛЕНИЯ ОРИЕНТАЦИИ СУСТАВА МАНИПУЛЯТОРА

В области мехатронных систем часто используются работы-манипуляторы для автоматизированной сборки изделий, сварки, окрашивания деталей и т.п. Важной задачей при этом является оптимизация времени движения по заданной траектории манипулятора. Для решения такой задачи необходимо не только точно оценить скорость движения узлов манипулятора, но и обеспечить линейную характеристику оценки позиции механизма в широком диапазоне изменения скоростей. **Предметом** исследования в статье являются методы определения ориентации сустава манипулятора. **Цель** работы – разработка модуля для определения ориентации сустава манипулятора и исследования его работы с целью определения пригодности конструкции для практического использования. В статье решаются следующие **задачи:** исследовать принципы определения ориентации суставов промышленных роботов; выбрать конструкцию модуля определения ориентации; разработать алгоритм определения позиции сустава в любое время; выполнить экспериментальные исследования работы модуля определения позиции с целью подтверждения пригодности конструкции для практического использования. Используются следующие **методы:** экспериментальные исследования проводились на реальном объекте – модели сустава робота-манипулятора, созданного с помощью методов и средств 3D-прототипирования; для определения положения сустава манипулятора использовались методы обработки сигналов, полученных от датчиков; обработка результатов экспериментов и расчет погрешностей позиционирования сустава манипулятора основываются на методах статистического анализа случайных величин. Получены следующие **результаты:** исследованы принципы определения ориентации суставов промышленных роботов; разработана конструкция и создан модуль определения ориентации сустава манипулятора; разработан алгоритм определения позиции сустава в любое время; экспериментально подтверждена пригодность конструкции для практического использования. **Выводы:** в данной работе предложены два варианта конструкции датчика для определения абсолютного угла поворота сустава манипулятора: резистивный и магнитный. Предложенная конструкция резистивного датчика оказалась нетехнологичной и намного больше по размерам, чем конструкция магнитного датчика. Полученные в процессе проведения экспериментальных исследований предлагаемого метода измерения угла поворота механического редуктора сустава манипулятора данные свидетельствуют о точном определении угла с помощью магнитного датчика. Рассчитанная погрешность измерений составляла менее 1,4 градуса. Также результаты эксперимента показали, что помимо радиального направления движения редуктора сустава манипулятора происходит существенное смещение вдоль рабочей плоскости, причем в некоторых случаях такие смещения носят хаотический характер. Это обуславливается некоторыми дефектами и несовершенством поверхности изготовленных деталей модели сустава, которые использовались в исследованиях.

Ключевые слова: манипулятор; позиционирование; ориентация; угловое вращение; проектирование; промышленный робот.

Бібліографічні описи / Bibliographic descriptions

Невлюдов І. Ш., Новоселов С. П., Сичова О. В. Розробка модуля визначення орієнтації суглоба маніпулятора і дослідження його роботи. *Сучасний стан наукових досліджень та технологій в промисловості.* 2022. № 2 (20). С. 86–96. DOI: https://doi.org/10.30837/ITSSI.2022.20.086

Nevlyudov, I., Novoselov, S., Sychova, O. (2022), "Development and study of the operation of the module for determining the orientation of the manipulator joint", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 86–96. DOI: https://doi.org/10.30837/ITSSI.2022.20.086

Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20) *ISSN 2522-9818 (print)* *ISSN 2524-2296 (online)*

UDC 004.896 DOI: https://doi.org/10.30837/ITSSI.2022.20.097

I. NEVLIUDOV, O. TSYMBAL, A. BRONNIKOV

INFORMATION MODELS FOR MANUFACTURING WORKSPACES IN ROBOTIC PROJECTS

The **subject** of research in the article are the workspace models for flexible integrated robotic systems. The **goal** of the work is in development of information models to represent workspaces for following application in the automated control systems of flexible integrated manufacturing. The article solves the next **tasks:** to analyze the representation of workspace to decide practical problems of robotic systems of different nature, to consider the development of informational models for representation on workspaces of intelligent control systems of integrated manufacturing, to consider the practical examples of information presentation on workspaces of production systems. Research **methods** are set theory and predicate theory. The following **results** were obtained: there were analysed the main features of informational models development to solve robotic tasks of different nature and were pointed the limitations of existing approaches of formal description, the need of integration of workspace models to decision-support systems and systems of graphical and mathematical simulation of integrated systems; the set theory-based model of information representation for problem-solving processes of flexible integrated robotic systems is proposed; the information-logic model of workspace for mobile robot applications, functioning in flexible integrated systems. is developed and contains the list of objects, includes their geometrical dimensions and supplies the preservation of parameters in time and space; information presentation for automated control system of flexible integrated manufacturing, which implements proposed models, is considered. **Conclusions:** application of models of information type for automated control systems makes to supply logical unification of flexible integrated manufacturing elements, to provide monitoring of states of technological equipment of production systems in space and time and formation of their digital twins, to promote functioning of intelligent decision-support systems for robotic systems of different types, that improves characteristics of production control.

Keywords: information model; workspace; mobile robot; flexible integrated system.

Introduction

While Industry 4.0 as a concept of economy and society development quit recently celebrated its 10th anniversary in 2021 [1], the implementation of this concept still doesn't cover a lot of different fields. Successful examples of Industry 4.0 applications first of all connected to creation of new manufacturing units, which incorporate novel production ideas just from first step. Another case is for elderly production areas with their existing structure, logistics, equipment, and services. They can become great attention points for Industry 4.0 applications to get new impacts to production processes and to achieve new sufficient levels without huger investments, compared to creations of new manufacturing units.

Simultaneously, application of new industrial concepts defines huge rise of information on every production element and its numerous connections to other elements. At the level of model, each parameter of the system must be taken in account. In these conditions, development of informational models becomes important but routine procedures for manufacturing systems simulation and development. Such simulation of manufacturing objects makes essentially real the idea of digital twins for any element of flexible systems.

Current article considers approaches to build informational models of workspaces for flexible integrated robotic systems, for the following support of intelligent decision-making systems of robots, also to support concept of digital twins of manufacturing units.

1. Analyses of existing approaches for robotic workspace presentation

Simulation and presentation of robotics workspaces started many years before appearance of current manufacturing concepts, for example, in STRIPS problem solver [2] the workspace (WS) of an intelligent robot was described as a set of predicate-described facts, connecting static and dynamic properties of WS areas, position of robot and object of production process. Other approach, described in [3] deals with same ideas as STRIPS but for Human Robotic Collaborative workspace, divided into passive resources (working tables, fixtures etc.) and active resources (humans and robots) given a task and secondly, with the number and type of active resources to be selected for a task. Thus, authors of [3] propose to organize WS in form of facts and actions with estimation of floor spaces, reachability of robotic resources, ergonomics, and investments (see fig. 1), while with minor formal description of WS properties.

In [4] authors consider human-robot collaboration for adaptive autonomous systems, including robot assistants. They consider human-robot team as a Markov decision process (MDP), with states of robotic world (WS) $x \in X$, robotic actions $a^R \in A^R$, and human actions $a^H \in A^H$. The proposed decision-making system evolves according to a probabilistic state transition function $p\left(x' \mid x, a^R, a^H\right)$, that specifies the probability of transitioning from state *x* to state *x*`, when actions a^R and a^H are applied in state *x*. Also, [4] proposes to store the history of interactions between robot and human in time.

Research in [5] suggest to look at manipulation of robotic systems as a knowledge-based system, supported by skills and presents a method for automatically generating planning problems from existing skill definitions such that the resulting problems can be solved using off-the-shelf planning software, and the solutions can be used to control robot actions in the world. The key role for robotic WS representation here is provided by

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

SkiROS and its world model. According to [6] The world state is partially predefined by a human operator in the ontology, partially abstracted from the robot by perception, and completed with the procedural knowledge embedded in the skills and primitives, that is shown in figure 2.

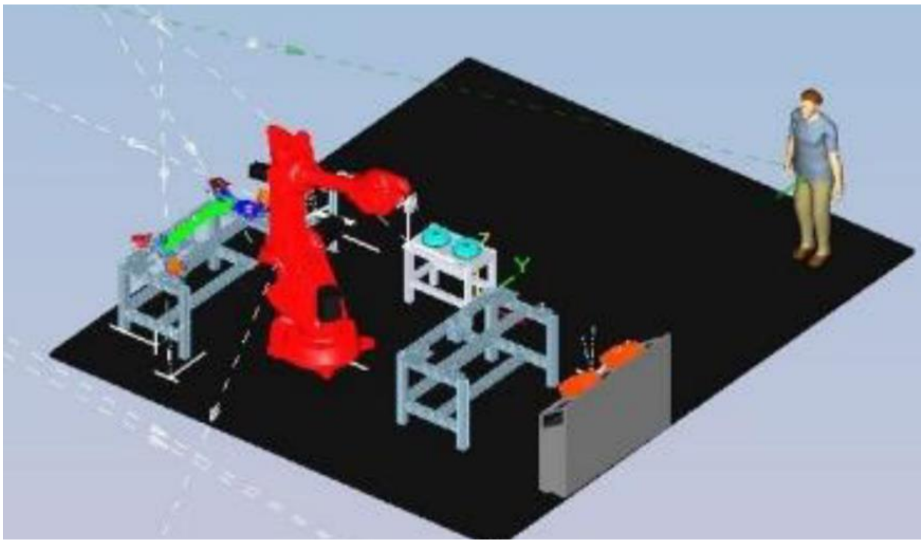


Fig. 1. Optimized workspace layout for manufacturing robotic cell [3]

Article [7] considers knowledge presentation of robotics systems from different levels: abstraction of low-level features (features that can be acquired by a robotic system) with high-level knowledge that can be interpreted by humans, described as skills. Transfer of skills (manipulations) is provided by demonstration of human actions and next imitation of them by the robot manipulator. Problems of robotic system workspaces presentation are also discussed in [8 - 10].

For instance, [8 - 9] proposes the formal description of data for robot's automated control system (ACS). ACS from strategies planning viewpoint is depicted by sets:

Robotic technical system (RTS as part of FIS), with states of set $x_i \in X, i = 0...n-1$, is a vector of states $X = \left\{X^0, X^1, \ldots, X^{n-1}\right\}$, that at time moments $t_0, \ldots, t_{n-1}$ has values $X_0 = \left\{x_0^0, x_0^1, \ldots, x_0^{n-1}\right\}$, $X_1 = \left\{x_1^0, x_1^1, \ldots, x_1^{n-1}\right\}, \ldots,$ $X_{n-1} = \left\{x_{n-1}^0, x_{n-1}^1, \ldots, x_{n-1}^{n-1}\right\}$.

RTS exists in a workspace (WS) $s_i \in S, i = 0...m-1$.

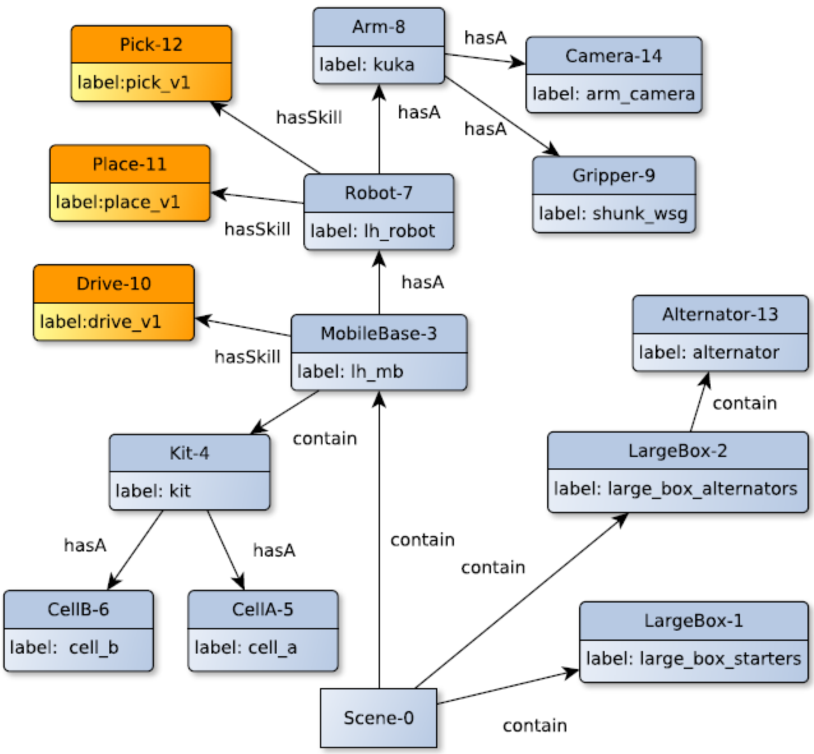


Fig. 2. World model instance for physical (blue) and abstract (orange) objects in [5]

Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

WS is 2-dimensional or 3-dimensional and depends of time. The set of specifications of WS is given as vector of states $S=\{S^0,S^1,\ldots,S^{n-1}\}$ and at the time moments $t_0,\ldots,t_{n-1}$ has the values $S_0=\{s_0^0,s_0^1,\ldots,s_0^{n-1}\}$, $S_1=\{s_1^0,s_1^1,\ldots,s_1^{n-1}\}$,…, $S_{n-1}=\{s_{n-1}^0,s_{n-1}^1,\ldots,s_{n-1}^{n-1}\}$;

RTS can generate decisions $d_k\in D, k=0...l-1$ on transformation of its states and states of WS. The set of decisions, generated by strategies planning system (SPS) defines vector $\vec{D}=\{d_0,d_1,\ldots,d_{m-1}\}$, with m – the number of decisions for times $t_0,\ldots,t_{n-1}$;

Decisions are implemented by RTS actions: $a_i\in A, i=0...l-1$.

The set of actions $A=\{a^0,a^1,\ldots,a^{n-1}\}$ is executed by RTS as implementation of found decisions $\vec{D}_i$ with subsets of movements or manipulations $a_{mv}\subset A$, $a_{mp}\subset A$.

The purpose of RTS functioning is a state $y\in X$, which is reached by sequential states transitions: $x_0\to x_1\to\ldots\to x_{n-1}=y$.

Therefore at process of target achievement there are transformations:

$$x_1 = f_1(x_0,y,s_0,d_0,a_0)+\varepsilon_0,\quad \|x_1-x_0\|\le\varepsilon_0,$$

………………………………..

$$x_k = f_k(x_{k-1},y,s_{k-1},d_{k-1},a_{k-1})+\varepsilon_k,\quad \|x_k-x_{k-1}\|\le\varepsilon_k,$$

………………………………..

$$y = f_n(x_{n-1},y,s_{n-1},d_{n-1},a_{n-1})+\varepsilon_n,\quad \|y-x_{n-1}\|\le\varepsilon_n,$$

f – transition function, ε – transition error.

Transitions are described by cost $c_i\in A, i=1...n$ and duration $t_i\in T, i=1...n$. The aim is to find such sequence of transitions $f_1,\ldots,f_n$, which will supply the system transition from initial state x_0 to purpose y.

Conditions of search are: $\sum_{i=1}^{n}t_i\to\min$, $\sum_{i=1}^{n}c_i\to\min$, $\sum_{i=1}^{n}\varepsilon_i\to\min$.

The mentioned sets present the real elements of ACS and provide information support for decision-making system of mobile or manipulation robots, acting as a part of flexible integrated production system.

2. Information-logical model of mobile robot workspace

The creation of any control objects model is impossible without a workspace model in which there are such objects that perform their tasks [11 - 13].

Let us consider the construction of a workspace model of a flexible integrated manufacturing system (FIMS), in which the tasks of mobile robot control are set.

Let there be a workspace W_s of robot Rb. Workspace is described by properties:

- geometric dimensions $D(x,y,z)$;
- a set of space-belonging objects Obj;
- time interval T_{param} of WS existence.

Then the space can be written as follows:

$$W_s=<D(x,y,z),Obj,T_{param}> \tag{1}$$

Each of the objects of the WS objects set Obj has a unique identifier ID, which means the ability to identify the object, using barcodes, QR codes, etc.

It is necessary to consider the main property of space – its discreteness and finiteness (limitedness). By finiteness we mean the limits of the camera working space. The case of opened (unlimited) space is, in principle, a separate problem.

By discreteness, we mean the division of space into cells that are the same in length and width. Depending on the WS discretization level, it is possible to set the tasks of moving (or manipulating) control objects of different accuracy.

The discrete nature of the working space means the presence of the coordinates of objects located in the WS and the occupancy factor of the WS section:

$$D(z,y,z)=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}d(x_i,y_j,z_k),\ K_{FL}\in[0,1], \tag{2}$$

where $d(x_i,y_j,z_k)$ – geometric parameters of a discrete space cell, K_{FL} – cell fill coefficient. All cell parameters must be the same size.

$$K_{FL}=\frac{S_{FL}(d(x,y,z))}{S(d(x,y,z))},K_{FL}\le 0.25, \tag{3}$$

where $S(d(x,y,z))$ – discrete space cell area, $S_{FL}(d(x,y,z))$ – filled part of discrete space cell $d(x,y,z)$.

The FIMS workspace assumes the existence of certain objects Obj – verstats (Vr), instrument (Ins), equipment (Osn), humans (Hum), robot (Rb), storages ($Storage$), conveyors ($Conv$), workspace monitoring devices (Mon):

$$\begin{gathered}\exists Vr\in W_s;\exists Ins\in W_s;\exists Osn\in W_s;\exists Hum\in W_s;\exists Rb\in W_s;\\ \exists Storage\in W_s;\exists Conv\in W_s;\exists Mon\in W_s\end{gathered} \tag{4}$$

$$Obj=<Vr,Ins,Osn,Hum,Rb,Storage,Conv,Mon>. \tag{5}$$

It follows from this that, from the point of view of property declaration, the entire GIVS can be expressed by the expression:

$$FIS=<W_s,Rb,Vr,Ins,Osn,Hum,Storage,Conv,Mon>. \tag{6}$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

Each of the objects owns a set of parameters. These properties have specific values, are included in a set of property names and values. Table 1 shows the main characteristics of objects in the symbolic representation.

There are ownership relations between objects (objects) and their properties, that is, certain properties belong to a certain object. An example of the properties of objects is also presented in table 1.

An example of the scheme of the workspace and the objects in it is shown in fig. 3, which shows the need to consider the human factor when planning transportation operations for mobile robots.

Workspace objects W_s exist both statically and dynamically.

The following objects can be carried to the static objects, which do not change the position and do not influence states of the robot movement: verstats (Vr), conveyors ($Conv$) and storages ($Storage$).

Dynamic objects that can change their position and thereby affect the movement state in the workspace are: instruments (Ins), equipment (Osn), humans (Hum).

Observation of the dynamics of the working space is provided by monitoring devices, which include object systems of computer / technical vision (OVSC) – $Camera_{Glob}$ and local computer / technical vision systems (LVSC) – $Camera_{Loc}$, other workspace status sensors ($Sens$).

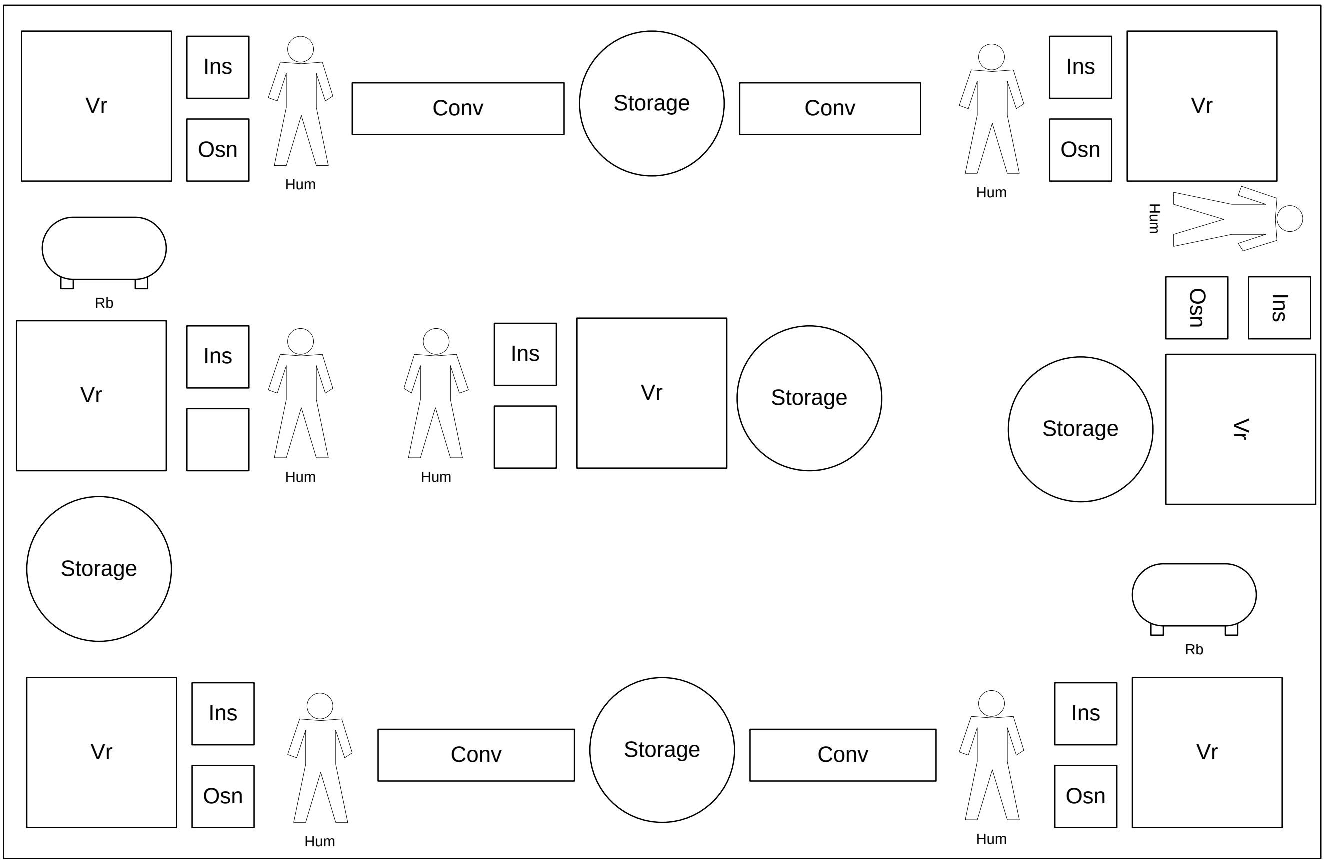


Fig. 3. An example of the objects locations in the workspace

Table 1. *List of objects* Obj *properties*

Object	Object property $Param_{Obj}$	Property name indication
Vr	Verstat type	$Type_{Vr}$
	Geometric parameters	$D_{Vr}(x_{Vr}, y_{Vr}, z_{Vr})$
	Processing methods	PM_{Vr}
	Special conditions	Sc_{Vr}
	Unique identifier	ID_{Vr}
Ins	Instrument type	$Type_{Ins}$
	Geometric parameters	$D_{Ins}(x_{Ins}, y_{Ins}, z_{Ins})$
	Processing methods	PM_{Ins}
	Unique identifier	ID_{Ins}

Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

The end **Table 1.**

Osn	Equipment type	$Type_{Osn}$
	Geometric parameters	$D_{Osn}(x_{Osn}, y_{Osn}, z_{Osn})$
	Unique identifier	ID_{Osn}
Mon	OVSC	$Camera_{Glob}$
	LVSC	$Camera_{Loc}$
	Other sensors	$Sens$
Hum	Geometric parameters	$D_{Hum}(x_{Hum}, y_{Hum}, z_{Hum})$
	Movement parameters in workspace	$Mv_{Hum}(x_{HumMv}, y_{HumMv}, z_{HumMv})$
	Belonging to the staff	Per_{Hum}
	Experience	Exp_{Hum}
	Age	Age_{Hum}
	Quality	$Qual_{Hum}$
	Unique identifier	ID_{Hum}
Rb	Geometric parameters	$D_{Rb}(x_{Rb}, y_{Rb}, z_{Rb})$
	Movement parameters in workspace	$Mv_{Rb}(x_{Rb}, y_{Rb}, z_{Rb})$
	Movement speed	$Speed_{Rb}$
	Current position	$Cp_{Rb}(x_{cpRb}, y_{cpRb}, z_{cpRb})$
	Unique identifier	ID_{Rb}
Object	Object property $Param_{Obj}$	Property name indication
Storage	Geometric parameters	$D_{Storage}(x_{Storage}, y_{Storage}, z_{Storage})$
	Type	$Type_{Storage}$
	Quantity of parts	$Quan_{Storage}$
	Unique identifier	$ID_{Storage}$
Conv	Geometric parameters	$D_{Conv}(x_{Conv}, y_{Conv}, z_{Conv})$
	Type	$Type_{Conv}$
	Quantity of parts	$Quan_{Conv}$
	Speed	$Speed_{Conv}$
	Unique identifier	ID_{Conv}

According to table 1, all properties of objects can be written in the form of tuples of parameters.

$$\forall v \in Vr, \exists v = < Type_{Vr}, D_{Vr}(x_{Vr}, y_{Vr}, z_{Vr}), PM_{Vr}, Sc_{Vr}, ID_{Vr} > \quad (7)$$

$$\forall ins \in Ins, \exists ins = < Type_{Ins}, D_{Ins}(x_{Ins}, y_{Ins}, z_{Ins}), PM_{Vr}, ID_{Ins} > \quad (8)$$

$$\forall o \in Osn, \exists o = < Type_{Osn}, D_{Osn}(x_{Osn}, y_{Osn}, z_{Osn}), ID_{Osn} > \quad (9)$$

$$\forall h \in Hum, \exists h = < D_{Vr}(x_{Vr}, y_{Vr}, z_{Vr}), Mv_{Hum}(x_{HumMv}, y_{HumMv}, z_{HumMv}), Per_{Hum}, Exp_{Hum}, Age_{Hum}, Qual_{Hum}, ID_{Hum} > \quad (10)$$

$$\forall rb \in Rb, \exists rb = < D_{Rb}(x_{Rb}, y_{Rb}, z_{Rb}), Mv_{Rb}(x_{Rb}, y_{Rb}, z_{Rb}), Speed_{Rb}, Cp_{Rb}(x_{cpRb}, y_{cpRb}, z_{cpRb}), ID_{Rb} > \quad (11)$$

$$\forall storage \in Storage, \exists storage = < D_{Storage}(x_{Storage}, y_{Storage}, z_{Storage}), Type_{Storage}, Quan_{Storage}, ID_{Storage} > \quad (12)$$

$$\forall conv \in Conv, \exists conv = < D_{Conv}(x_{Conv}, y_{Conv}, z_{Conv}), Type_{Conv}, Quan_{Conv}, Speed_{Conv}, ID_{Conv} > \quad (13)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

$$\forall mon \in Mon, \exists mon =< Camera_{Glob}, Camera_{Loc}, Sens > . \quad (14)$$

At the same time, the monitoring system consists of surveillance cameras and sensors of various types and purposes.

Cameras have the following properties:

$$\forall cam \in Cam, \exists cam =< Inst_{pt}(x_{pt}, y_{pt}, z_{pt}), Angle_{View}, Resolution > . \quad (15)$$

All objects of the working space interact with each other by various kinds of dependencies, which allows us to introduce a definition.

Definition 1. Each workspace object has at least one property.

$$\forall x (x \in Obj) \exists param (param \in Param_{Obj})[x(param)], \quad (16)$$

where $\forall$ – general quantifier, $\exists$ – quantifier of existence, x – a WS specific object, Obj – set of WS objects, $Param_{Obj}$ – set of object parameters.

$Param_{Obj}$ set of objects properties includes parameters such as: $Param_{Vr}$ – set of verstats properties, $Param_{Ins}$ – set of intstruments properties, $Param_{Osn}$ – set of equipment properties, $Param_{Hum}$ – set of human poperties, $Param_{Rb}$ – set of robot properties, $Param_{Storage}$ – set of storage properties, $Param_{Conv}$ – set of conveyor properties, as described in table 1.

Hence:

$$\begin{gathered} Param_{Obj} = Param_{Vr} \cup Param_{Ins} \cup Param_{Osn} \cup \\ \cup Param_{Hum} \cup Param_{Rb} \cup Param_{Storage} \cup Param_{Conv} \end{gathered} . \quad (17)$$

From these definitions it follows that:

$$\forall x \exists Param_{Obj} [Param_{Vr}(x)], \quad (18)$$

$$\forall x \exists Param_{Obj} [Param_{Ins}(x)], \quad (19)$$

$$\forall x \exists Param_{Obj} [Param_{Osn}(x)], \quad (20)$$

$$\forall x \exists Param_{Obj} [Param_{Hum}(x)], \quad (21)$$

$$\forall x \exists Param_{Obj} [Param_{Rb}(x)], \quad (22)$$

$$\forall x \exists Param_{Obj} [Param_{Storage}(x)], \quad (23)$$

$$\forall x \exists Param_{Obj} [Param_{Conv}(x)]. \quad (24)$$

Definition 2. Each object of space relates to any object with another object:

$$\forall x \exists y (x \leftrightarrow y). \quad (25)$$

The definition is correct since each of the objects is designed to interact with other objects.

Definition 3. All FIMS workspace are ordered in relation to others:

$$\forall x \exists y, \{x,y\}. \quad (26)$$

Definition 4. For each item in the workspace, there is another item that is compatible with the first one in the process of work:

$$\forall x \exists y, x \cap y. \quad (27)$$

The definition is true since each of the robotic area objects exists in order to participate in the technological process.

Definition 5. There are such items that predetermine each other in the technological process.

$$\forall x \exists y, x \rightarrow y . \quad (28)$$

This relation is a special case of expression by definition 4, so it exists between the same objects.

Definition 6. There are the same objects.

$$\forall x \exists y \in x \equiv y . \quad (29)$$

Definition 7. For each property value $param_i$ there will be a match for him. Symbolically, this expression can be written as:

$$\forall param_i \exists param_j ([param_i] = [param_j]). \quad (30)$$

Definition 8. For each numerical value of a property (except for the maximum value on a finite set of values), you can find a value greater than the current one.

$$\forall param_i \exists param_j ([param_i] < [param_j], param_i \in N, param_j \in N) \quad (31)$$

In addition to the FIMS workspace, where the robot works, there is another one – the warehouse equipment space $Warehouse$, which interacts with the FIMS and has a set of characteristics, in particular geometric parameters $D_{Warehouse}(x_{Warehouse}, y_{Warehouse}, z_{Warehouse})$, materials (blanks, component parts and folding etc.) $Material$ and ready products $Product$, as well as transport parameters $Transport$.

$$Warehouse =< D_{Warehouse}(x_{Warehouse}, y_{Warehouse}, z_{Warehouse}), Material, Product, Transport > \quad (32)$$

In this model, the parameter $Material$ can be shown with a set of materials:

$$Material = (material_1, material_2, ..., material_n) . \quad (33)$$

Similarly for products and transportation parameters:

Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

$$Product = (product_1, product_2, ..., product_n), \quad (34)$$

$$Transport = (transport_1, transport_2, ..., transport_n). \quad (35)$$

Thus, all the introduced designations of the FIMS WS objects and the belonging transportation system form an information-logical model of the robotic system. The main purpose of the proposed model is to save current information about the state of FIMS objects and related systems, as well as to support the execution of queries about the objects properties that are included in the information-logical model description.

For example, for the workspace shown in fig. 1.5, the construction of an information-logical model will be formed based on the following input data.

There is a workspace with geometric dimensions of 70 x 25 x 10 m. It contains objects such as people, machines and equipment with various kinds of tools, storage, overhead stacker crane as a system for moving goods between two machines, or a machine and an equipment cabinet.

The machines used have certain overall dimensions (1.7 x 1.906 x 2.26 m for ANS machines, 1.78 x 2.2 x 1.675 m for ASM machines used in production).

Cabinets are equipped with geometric dimensions of 1.5 x 0.7 x 1.7 m. They contain both general purpose tools and specialized tools used on machine tools.

If the tool is heavy, then a stacker crane is used to move it between the tool cabinet and the machine (10 m).

Operations for changing the load, its movement, as well as tracking the machines are performed by a person.

After assembling the products, they are moved to the drives, from where a person, using a trolley, delivers them to the equipment warehouse.

It should be noted that the gaps between the objects of the workspace are very wide, and it is advisable to use mobile robots for transportation operations, which will significantly speed up the process.

Presentation of a flexible production site based on the developed model is shown in fig. 4.

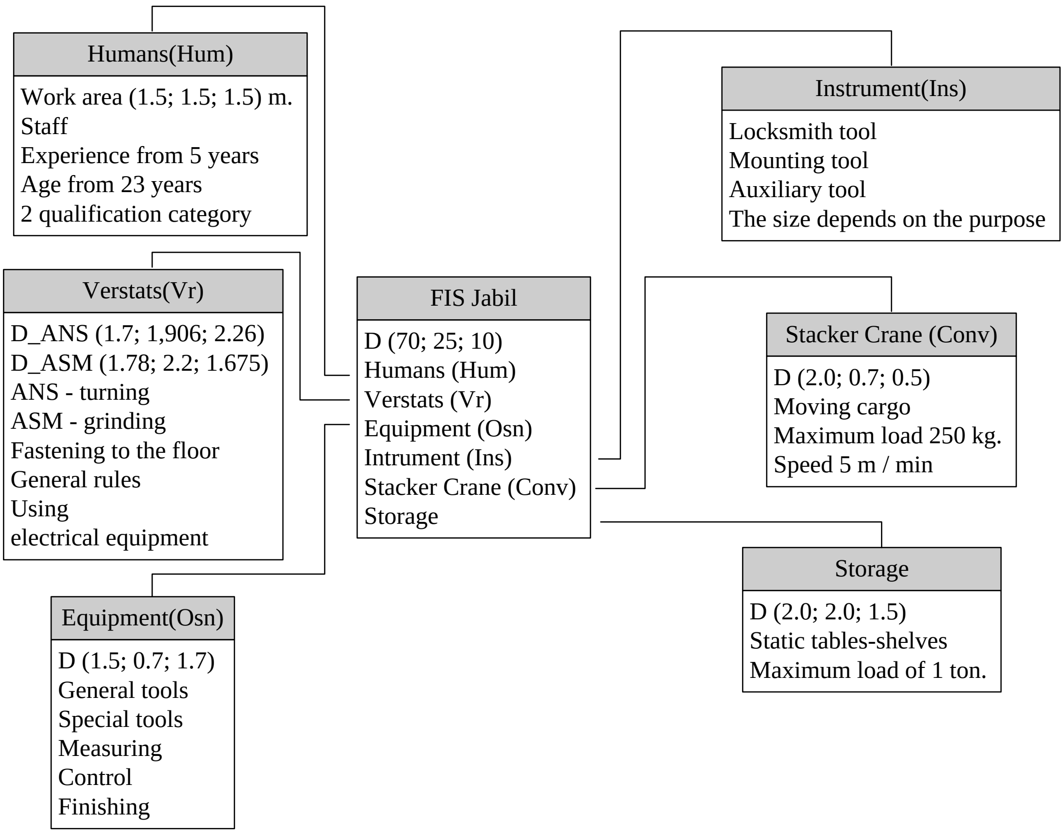


Fig. 4. Flexible production site based on the developed model

Proposed approach can describe basic properties of flexible manufacturing units, cells or areas. Composition of such descriptions can present background for development of automated control systems or their particular elements, including intelligent decision-making systems.

Conclusion

The actual problem of modern flexible integrated system (FIS), which follow the concept of Industry 4.0 is in large-scale supplement of informational support for production processes at all their stages. Such support can be supplied by introduction of information models, presenting elements of production systems. While consideration of robotic workspace models is still an actual task for researchers [11 - 13], new approaches, including visual sensoring [14 - 15] can give impacts to models of workspaces, especially in case of dynamic changes.

The FIS and robot's functioning in real-time mode also require information on production system, on robot

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

itself, on all surrounding objects, making workspace of manufacturing robot.

Proposed article makes an analysis of existing approaches to simulate robotics workspaces, contains description of workspace models of informational type, which can be used to supply functioning of automated control systems, of intelligent decision-making systems for robots and other elements of FIS. The results of this work were used to supply execution of scientific project “Multi-purpose robotic platform with advanced manipulation possibilities” in the Kharkiv National University of Radio Electronics.

References

1. Skitsko, V. (2016), "Industry 4.0 as the industrial production of the future" ["Industriya 4.0 yak promyslove vyrobnytstvo maybutn′oho"], *Investment: practice and experience*, Vol. №5/20, P. 33–40.
2. Haslum, Patrik (2007), "Reducing Accidental Complexity in Planning Problems", *Proceedings of the 20th International Joint Conference on Artificial Intelligence*, P. 1898–1903.
3. Tsarouchi, P., Spiliotopoulos, J., Michalos, G., Koukas, S., Athanasatos, A., Makris, S., Chryssolouris, G. (2016), "A Decision Making Framework for Human Robot Collaborative Workplace Generation", *Procedia CIRP*, Vol. 44, P. 228–232. **DOI:**https://doi.org/10.1016/j.procir.2016.02.103.
4. Chen, M., Nikolaidis, S., Soh, H., Hsu, D., & Srinivasa, S. (2020), "Trust-aware decision making for human-robot collaboration: Model learning and planning", *ACM Transactions on Human-Robot Interaction (THRI)*, 9 (2), P. 1–23. **DOI:**https://doi.org/10.48550/arXiv.1801.04099.
5. Upadhyay, J., Rawat, A., Deb, D., Muresan, V., Unguresan, M.-L. (2020), "An RSSI-Based Localization, Path Planning and Computer Vision-Based Decision Making Robotic System", *Electronics*, 9, P. 1326. **DOI:** https://doi.org/10.3390/electronics9081326.
6. Crosby, M., Rovida, F., Pedersen, M.- Rath, Petrick, Ronald P. A., Krüger, Volker (2016), "Planning for Robots with Skills", *Proceedings of the 4th Workshop on Planning and Robotics (PlanRob)*, ICAPS, P. 49–57.
7. Paulius, D., & Sun, Y. (2019), "A Survey of Knowledge Representation in Service Robotics", *Robotics Auton. Syst*., 118, P. 13–30.
8. Tsymbal, A., Bronnikov, A., Yerokhin, A. (2019), "Adaptive Decision-making for Robotic adaptive tasks", *Proceedings of IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL)*, Sozopol, Bulgaria, 6–8 Sept., P. 594–597, **DOI:** https://doi:10.1109/CAOL46282.2019.9019488.
9. Tsymbal, O., Mercorelli, P., Sergiyenko, O. (2021), "Predicate-Based Model of Problem-Solving for Robotic Actions Planning", *Mathematics*, 9 (23), P. 3044.
10. Tsymbal, O. M., Bronnikov, A. I., Kutsenko, O. I., Shein, E. S. (2014), "The concept of intelligent production agents and features of its implementation" ["Kontseptsiya intelektual′nykh vyrobnychykh ahentiv ta osoblyvosti yiyi realizatsiyi"], *Eastern European Journal of Advanced Technologies*, Kharkov, No. 1/2 (67), P. 9–13.
11. Honjwei, M., Longlong, M. (2012),"Robot Path Planning Based on Differential Evolution in Static Environment", *International Journal of Digital Content Technology and its Applications (JDCTA)*, Vol. 6, No. 20, P. 122–129.
12. Khor, A., Yong, A. (2018), "Robotics in Supply chain, in: L. Huan, S. Raman (Eds.), Emerging Trends of Technologies in Supply Chain Management", *WOU Press*, P. 25–38.
13. Mikhailov, E.; Remenyuk, B. (2015), "Optimize the placement warehouse transport system", *J. Electrotech. Comput. Syst*., 18, P. 60–64.
14. Sergiyenko, O., Flores-Fuentes, W., Mercorelli, P, Eds. (2019),"Machine Vision and Navigation", *Springer*, Berlin/Heidelberg, Germany, 12 November; P. 851.
15. Sergiyenko, O. Y.; Tyrsa, V. V. (2021), "3D Optical Machine Vision Sensors With Intelligent Data Management for Robotic Swarm Navigation Improvement", *IEEE Sens., J.*, 21, P. 11262–11274.

Received 23.05.2022

Відомості про авторів / Сведения об авторах / About the Authors

Невлюдов Ігор Шакирович – професор, доктор технічних наук, Харківський національний університет радіоелектроніки, завідувач кафедри комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: igor.nevliudov@nure.ua; ORCID ID: https://orcid.org/0000-0002-9837-2309.

Невлюдов Игорь Шакирович – профессор, доктор технических наук, Харьковский национальный университет радиоэлектроники, заведующий кафедрой компьютерно-интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Nevlyudov Igor – Professor, Doctor of Engineering Sciences, Kharkiv National University of Radio Electronics, Head at the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

Цимбал Олександр Михайлович – доктор технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри комп’ютерно- інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: oleksandr.tsymbal@nure.ua; ORCID: 0000-0002-4947-7446.

Цымбал Александр Михайлович – доктор технических наук, доцент, Харьковский национальный университет радиоэлектроники, профессор кафедры компьютерно- интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Tsymbal Oleksandr – Doctor of Science (Engineering), Associate professor, Kharkiv National University of Radio Electronics, Professor of the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

Бронніков Артем Ігорович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри комп’ютерно-інтегрованих технологій, автоматизації та мехатроніки, м. Харків, Україна; e-mail: artem.bronnikov@nure.ua ; ORCID: https://orcid.org/0000-0003-3096-7653. Тел.: 057-7021486.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. №2 (20) ISSN 2524-2296 (online)

Бронников Артем Игоревич – кандидат технических наук, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерно-интегрированных технологий, автоматизации и мехатроники, г. Харьков, Украина.

Bronnikov Artem – Candidate of Technical Science, Kharkiv National University of Radio Electronics, Associate professor of the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv, Ukraine.

ІНФОРМАЦІЙНІ МОДЕЛІ ДЛЯ ВИРОБНИЧИХ РОБОЧИХ ПРОСТОРІВ У РОБОТОТЕХНІЧНИХ ПРОЕКТАХ

Предметом дослідження статті є моделі робочого простору гнучких інтегрованих роботизованих систем. **Мета** роботи – побудова інформаційних моделей представлення робочого простору з метою подальшого використання у автоматизованих системах керування гнучкого інтегрованого виробництва. В статті вирішуються наступні **завдання:** провести аналіз представлення робочого простору під час розв'язання практичних завдань роботизованих систем різного типу, розглянути побудову інформаційних моделей представлення робочого простору інтелектуальних систем керування інтегрованим виробництвом, розглянути практичні приклади представлення інформації про робочий простір виробничих систем. **Методами** дослідження є теорія множин та теорія предикатів. Отримано наступні **результати:** проаналізовано основні особливості побудови інформаційних моделей робочого простору для розвязання завдань робототехніки різного типу, вказується на обмеженість існуючих підходів формального опису, на необхідність інтеграції моделей робочого простору із системами підтримки прийняття рішень, системами графічного та математичного моделювання інтегрованих систем; запропоновано теоретико-множинну модель подання інформації щодо процесів прийняття ріщень у гнучких інтегрованих роботизованих системах; розроблено інформаційно-логічну модель робочого простору мобільного робота, яка містить перелік об'єктів, враховує їх геометричні розміри, забезпечує зберігання параметрів у часі та просторі; розглянуто подання інформації у автоматизованиій системі керування гнучкого інтегрованого виробництва, що реалізує запропоновані моделі. **Висновки:** застосування моделей інформаційного типу у автоматизованих системах керування дозволить логічно об`єднати елементи гнучкого інтегрованого виробництва, забезпечити моніторинг стану технологічного обладнання у робочому просторі виробничих систем та у часі, здійснити формування цифрових двійників елементів робочого простору, забезпечити функціонування інтелектуальних систем підтримки прийняття рішень роботизованих систем різного типу, що дозволить покращити характеристики процесів керування виробництвом.

Ключові слова: інформаційна модель; робочий простір; мобільний робот; гнучка інтегрована система.

ИНФОРМАЦИОННЫЕ МОДЕЛИ ДЛЯ ПРОИЗВОДСТВЕННЫХ РАБОЧИХ ПРОСТРАНСТВ В РОБОТОТЕХНИЧЕСКИХ ПРОЕКТАХ

Предметом исследования статьи являются модели рабочего пространства гибких встроенных роботизированных систем. **Цель** работы – построение информационных моделей представления рабочего пространства для дальнейшего использования в автоматизированных системах управления гибкого интегрированного производства. В статье решаются следующие **задачи:** провести анализ представления рабочего пространства при решении практических задач роботизированных систем разного типа, рассмотреть построение информационных моделей представления рабочего пространства интеллектуальных систем управления интегрированным производством, рассмотреть практические примеры представления информации о рабочем пространстве производственных систем. **Методами** исследования являются теория множеств и теория предикатов. Получены следующие **результаты:** проанализированы основные особенности построения информационных моделей рабочего пространства для решения задач робототехники разного типа, указывается на ограниченность существующих подходов формального описания, необходимость интеграции моделей рабочего пространства с системами поддержки принятия решений, системами графического и математического моделирования интегрированных систем; предложена теоретико-множественная модель представления информации о процессах принятия решений в гибких интегрированных роботизированных системах; разработана информационно-логическая модель рабочего пространства мобильного робота, которая содержит перечень объектов, учитывает их геометрические размеры, обеспечивает хранение параметров во времени и пространстве; рассмотрено представление информации в автоматизированной системе управления гибкого интегрированного производства, реализующей предлагаемые модели. **Выводы:** применение моделей информационного типа в автоматизированных системах управления позволит логически объединить элементы гибкого интегрированного производства, обеспечить мониторинг состояния технологического оборудования в рабочем пространстве производственных систем и во времени, осуществить формирование цифровых двойников элементов рабочего пространства, обеспечить функционирование интеллектуальных систем для принятия решений систем разного типа, что позволит улучшить характеристики процессов управления производством.

Ключевые слова: информационная модель; рабочее пространство; мобильный робот; гибкая интегрированная система.

Бібліографічні описи / Bibliographic descriptions

Невлюдов І. Ш., Цимбал О. М., Бронніков А. І. Інформаційні моделі для виробничих робочих просторів у робототехнічних проектах. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 97–105. DOI: https://doi.org/10.30837/ITSSI.2022.20.097

Nevliudov, I., Tsymbal, O., Bronnikov, A. (2022), "Information models for manufacturing workspaces in robotic projects", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 97–105. DOI: https://doi.org/10.30837/ITSSI.2022.20.097

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

UDC 623.6 DOI: https://doi.org/10.30837/ITSSI.2022.20.106

I. PAKHNYTS, S. KHRUSTALOVA, K. KHRUSTALEV

SYSTEM FOR DETECTION AND IDENTIFICATION OF POTENTIALLY EXPLOSIVE OBJECTS IN OPEN AREA

The **subject** of this research is the methods, means and systems for detecting potentially dangerous military objects in open terrain. The **purpose** of the study is to develop a system for the detection and identification of potentially explosive military objects using an unmanned aerial vehicle (drone), which includes a system for detecting an explosive object using a metal detector with the technology of adjusting the flight height and the detection method using a thermal imager. To achieve the goal, the following **tasks** were solved: a review and analysis of modern methods and systems for the detection and identification of potentially explosive military objects was carried out, the classification of identifiable explosive objects was determined, system components were selected, a structural diagram and an algorithm of the software control tool were developed system of identification of potentially explosive objects in an open area, a software tool for detection and identification of potentially explosive objects in an open area was created. The following **methods** are used in the work: the mathematical method of constructing cartographic grids, the method of recording infrared radiation, the method of eddy currents, methods and means of data collection and processing. The following **results** were obtained: the components of the system were selected, the structure, diagram and algorithm of the software tool for the identification of potentially explosive objects in the open area were developed, and the corresponding software was created. **Conclusions:** the application of the proposed system makes it possible to increase the accuracy of finding or the absence of a potentially explosive object in a certain area due to the use of two methods of detecting potentially explosive objects at once, and provides the opportunity to identify a sufficiently wide range of objects. The developed system is safe, as it is controlled by an operator who is at a safe distance, allows you to get special maps with terrain markings with information about the possible presence of potentially explosive objects in certain areas of the terrain and, in general, maps of metal detector and thermal imager signals.

Keywords: explosive object; mine; detection and identification system; drone; thermal imager; metal detector.

Introduction

Today, in the difficult conditions of martial law for Ukraine, it is important to preserve the lives and health of citizens who are returning to the territories that were under temporary occupation. Explosive military facilities pose a great threat. According to the spokesperson of the Ministry of Internal Affairs of Ukraine Alyona Matveeva the most common cases of injury and death of civilians from explosive objects are explosions of automobile and agricultural transport on anti-tank mines; on unpaved roads and fields, also explosions in forest belts and green zone on anti-personnel mines; and – explosions as a result of careless handling of ammunition found in areas of military operations by citizens. The problem also arises where farmland is cultivated – often agricultural machinery collides with mines, resulting in various emergency events.

In today's realities, the population of Ukraine is increasingly faced with the need for careful compliance with certain safety rules for many objects: industrial facilities, pyrotechnics, household chemicals, energy, etc. At first glance, simple things can become very dangerous to life and health. Such things include potentially explosive objects.

Most objects do not need special knowledge for identification because they have special stickers, inscriptions and markings that identify the object as explosive. However, there are explosive objects that do not have special markings and can be intentionally concealed to cause greater harm to the life and health of the person who finds them. These are military explosive objects. Therefore, the problem of detecting and identifying potentially explosive objects in open areas, especially where the most fierce hostilities took place, is an urgent task.

Open areas outside cities pose a great danger. For example, many explosive objects can be hidden in fields and plains: unexploded mines, shells, abandoned ammunition, etc.

In order to identify and neutralize such objects, mankind creates more efficient and safer automated systems.

Analysis of recent research and publications.

Demining involves a comprehensive approach to the entire area where combat operations have taken place and includes a survey of the entire area, identifying areas of concern, identifying areas with mines and explosive remnants, and clearing them. After humanitarian demining, the terrain becomes fully suitable for civilian use.

In the scientific literature, considerable attention has been paid to the training of demining specialists [1], the technology of mine clearance [2, 3]. The problems of humanitarian demining in their works covered Bevz A.M., Tolkunov I.O. [4], Govduk A.V., and Polotay O.I. [5]. The issue of mine safety training of the population in the scientific literature is still unexplored.

Taking into account the rapid development of robotics in the sphere of the considered activity, mine clearance works have gained popularity [6 - 8]. There is a robot for observation and work on explosive objects (EO) tEODor and a series of robots Telemax. TEODor. It is considered a large demolition robot for police and military purposes. Its approximate cost is $750,000. It can be used universally as a basic tool for tasking, threat prevention, firefighting or industrial applications. Its strong arm and extremely high reliability make it the No. 1 choice for the most dangerous and difficult tasks around the world [9 - 13]. The Telemax series of robots includesTelemax

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

4x4, Pro, Hybrid, Plus, Recce. Works from telemax series have different types of chassis and manipulators; they are specialized for individual tasks and can be used universally.All (except telemax RECCE) have a manipulator with Point Center Control tool for gripping objects with tongues, a tool magazine with automatic tool change and countless pre-programmed motion sequences. A wide range of accessories suitable for all telemax robots allows adaptation to a wide range of applications and specific tasks. Telemax 4x4: the wheeled version with a wide wheelbase and 4x4 drive for fast tasks on difficult terrain or loose ground. Telemax HYBRID, PRO and PLUS are similar models, characterized by the combination of the arm and different size of the "body" of the robot. Telemax RECCE is a compact and powerful reconnaissance system without a robot arm, which provides detailed information about the location of the necessary objects, especially when combined with a module creating 3D maps of the area. The most popular of the Telemax series of robots in "demining work" is Telemax PRO. Unlike the tEODor robot, Telemax: is equipped with a seven-axis manipulator, which is more maneuverable, allowing it to perform more delicate work, but with a smaller payload (up to 20 kg). A. Yakovlev and A. Parfilo note that to detect and neutralize explosive objects it is advisable to use robotic complexes such as "CALIBER MK4 Large EOD" from "ICOR Technology Inc." or 510 PackBot or even 710 Kobra from Endeavor Robotics. With their help, the operator can from a safe distance not only photograph the object and record video, but also remove traces of biological origin, which could belong to the person equipping and/or installing the EO [14].

Research material and results.

Explosive military objects that can threaten the lives of citizens returning to temporarily occupied territories can be divided into two types: mines and unexploded high-explosive shells.

Mines began to be used centuries ago and were surface or underground devices made of wood, explosives and triggers. To date, mines have been modernized simultaneously with other weapons and have a wide variety of materials, shapes, active ingredients, methods of use, etc. (fig. 1). According to the results of the study of open sources, modern mines can be divided into several types according to different categories:

- by tactical purpose: anti-tank, anti-personnel, anti-vehicle (road), anti-submarine, trap mines;
- by damage effect: blast wave, cumulative, fragmentation, shrapnel, thermal and others;
- by the principle of operation: controlled and automatic;
- by method of actuation: push, pull (tension), sentry and combined action;
- by the time of action: instantaneous action mines and delayed action mines;
- by body material: metal, plastic, wood, paper, glass and without body (of stamped explosives);
- by mounting level: suspended (mounted) above human height (above tank turrets, vehicle cabins); at ground level (human silhouette, vehicles, armored vehicles); buried in the ground (embedded in buildings or technical installations); mounted at the bottom of bodies of water or underwater part of a shore; floating in water
- by type of active substance;

Unexploded landmines can include projectiles that have been fired but have not detonated or ruptured for any reason. They are most often found up to 1 m deep near the ground or on the surface of the ground. They are dangerous because they can detonate and explode at any moment.

Fig.1. Types of mines and shells and their brief description

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

Special teams consisting of sappers of the Armed Forces of Ukraine and pyrotechnicians of the State Emergency Service carry out mine clearance work. The process of searching for potentially explosive objects differs for some types of objects.

For different methods of searching for unexploded ordnance, only two factors matter: the material of the ordnance and the active substance.

With mines, the situation is different: based on the types into which mines are divided, we can conclude that not all of these criteria are worth considering more carefully. It is therefore possible to distinguish the main criteria by which the search will be made:

1. By mode of actuation, by the material of the body;
2. By level of installation;
3. By type of active ingredient.

In 1881. Alexander Graham Bell invented the metal detector [15], which is now used for more thorough decontamination of large areas. It is possible to detect metal products in the ground by electrical conductivity. The detector works according to the following principle: a coil generates electromagnetic waves of a certain frequency, reflected from the sought target. The electronic unit processes the reflected wave and signals the detection of a metal object. Not all metals have the same electrical conductivity. This parameter allows you to understand what material the object is made of, even before digging. Most often, but not always when it comes to mines, there are mines of the same type in the same field. Therefore, when you manage to find one, you can find others by similar indicators. The advantages of the method include the accuracy and care for the area, but a significant disadvantage is the direct involvement in the search for the object and a very high cost of error for the health and the sapper, because some mines can react to changes in the magnetic field.

In the present, people have involved animals in the search for potentially explosive objects: dogs and rats. For the animal, it all looks like a game, but for sappers-cynologists it is a safer and faster method than using metal detectors. The disadvantages include the following: the quality and speed of detecting objects depends on the animal's mood, its relationship with the cyno-sapper and the ability to resist distractions.

Some experts argue that there are still no flawless solutions using automation, in particular drones to search for explosive objects. Technology is not yet able to say with absolute certainty that it has found a mine or a shell, but solutions already in the making make the detection process much easier and make it as safe as possible for both the sapper operator and the average person. The autonomy of drones and robots makes it possible to conduct search operations on the ground, with operators and sappers at a safe distance watching the process with the help of control devices.

Drones and search robots include those that have special devices with which a software tool or operator can determine the location of the explosive object with a certain accuracy. Such devices include thermal imager, metal detector and GPR [16, 17]. The advantages of such robotic systems include almost complete safety of the operator. To disadvantages - speed and accuracy of search, as almost always the results of search of drones and robots require verification by the operator-sapper, because they can react to almost any similar object, which is not explosive.

Modernity offers a great variety of solutions using robots and drones. Now they are not so effective as to completely replace humans, but they are already useful enough to be used in humanitarian missions.

Drones with thermal imagers are used to detect mines that are almost entirely made of plastic. Such systems take advantage of plastic's ability to heat up or mature more slowly than the environment, such as sand. Even if they are covered by soil, the difference in temperature will cause the rock above the object to be noticeably cooler or warmer than the rock around it. The difference stands out best in the morning and evening. Such objects are very difficult to detect with a metal detector, although they have elements of metal in their structure, but they can easily be confused with trash, bullets, shrapnel and other small elements of metal. At the same time, there is a significant disadvantage of using only a thermal imager: If the object is under the ground or other heated longer or at the same speed as the object to be found, this method of search does not make any sense, because on the thermal imager screen the difference will not be noticeable. The time of day also plays an important role, because during the day and at night this method almost does not give the necessary results.

Another example is the use of drones and robots with a metal detector to search for explosive objects. Sometimes GPR is added to such systems, which is not advisable to use in conditions where it is not known exactly what objects are to be found. In general, flying drones and works riding on a tracked platform are used. Works relatively not expensive, fast and accurate, but if you need to find explosive objects in areas with difficult terrain, in which the positioning of the robot will not be accurate enough, it is advisable to use flying drones.

For more efficient and safe operation, it is advisable to develop a system using a drone that includes a detection system with a metal detector with flight altitude adjustment technology and a detection method using a thermal imager. To control the proposed system of detection of potentially explosive objects requires the development of a software tool.

Research results and their discussion.

The proposed system for detecting and identifying potentially explosive objects in open terrain consists of the following components:

1. Drone with accelerometer and gyroscope.
2. A metal detector for the drone.
3. A digital thermal imaging camera for the drone.
4. A regular resolution camera.
5. Smartphone to control the system.

The structural diagram of the system for detection and identification of potentially explosive objects in an open area is shown in figure 2.

Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2522-9818 (print) ISSN 2524-2296 (online)

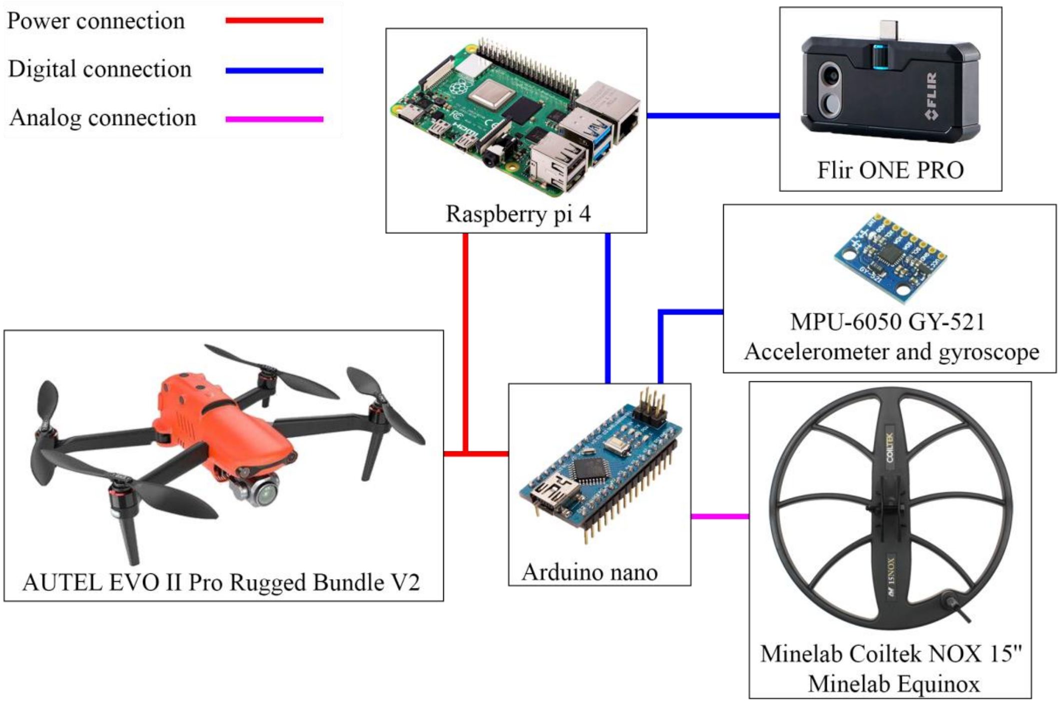


Fig. 2. Structural scheme of the detection and identification of potentially explosive objects in open areas

The proposed system consists of a computing device, sensors and a platform through which the system moves. The platform chosen is the AUTEL EVO II Pro Rugged Bundle V2 drone, which is reliable in terms of stabilization and ability to lift the entire system with a small margin. The selected drone platform has the ability to lift up to three kilograms of cargo and a flight time margin of up to 40 minutes. A metal detector and a thermal imager are needed to detect explosive objects. As a metal detector is used depth coil MinelabCoiltek NOX 15" Minelab Equinox, which weighs 890 grams. For thermal imaging was selected Flir one PRO, because it has a low weight, connection via Type C and a built-in camera used for the operation of the system. A computing device in the form of a Raspberry pi 4 mobile computer was chosen. The Raspberry Pi 4 computer is lightweight and has various digital interfaces, which are used to process data from the sensors and transfer it to the operator. The Raspberry Pi 4 has only digital ports, so the system comes with Arduino Nano, which has enough processing power to process signals from the coil of the metal detector. The gyroscope and accelerometer are built into the MPU-6050 GY-521 modules, used to calculate the movement and connected to the Arduino Nano board. The power of the system is connected to the power system of the drone itself or can be a separate element in the form of three lithium-ion batteries. First of all, the power is supplied to the Arduino Nano and Raspberry pi boards. Power for the thermal imager and camera is supplied from the Raspberry pi, power for the coil and the twin gyroscope and accelerometer module is supplied from the arduino nano.

A software tool was developed to control the proposed potentially explosive object identification system, the algorithm of which is shown in fig. 3.

To start working, it is necessary to select the mode of action of the thermal imager, depending on the time and weather conditions. During the flight, the software tool analyzes the output signals from the thermal imager, the data collector and sensors (gyroscope and accelerometer). After each interrogation, according to a certain algorithm, the map data is restored in certain areas where the scanning is performed.

The electrical conductivity of the area is different from the electrical conductivity of the ground.

Once the map is complete, the analysis of the map begins. During the analysis, according to the data received from the metal detector and thermal imager, areas with a higher probability of the presence of a potentially explosive object are determined. As a result of the work, the operator receives a map of the area with detected areas, signal maps of the metal detector and thermal camera.

Conclusions

Thus, the proposed system of identification of potentially explosive objects in the open terrain due to the premature use of metal detector with the technology of correcting the flight altitude and the method of detection using thermal imager allowed with high accuracy to identify a wide range of objects, also the system is safe for the operator.

Safety is understood to mean that the operator, who is at a safe distance, controls the drone. At the end of the terrain check, the operator receives a map containing terrain marks with information about the possible presence of potentially explosive objects in certain areas of the terrain and in general, the signal maps of the metal detector and thermal camera.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

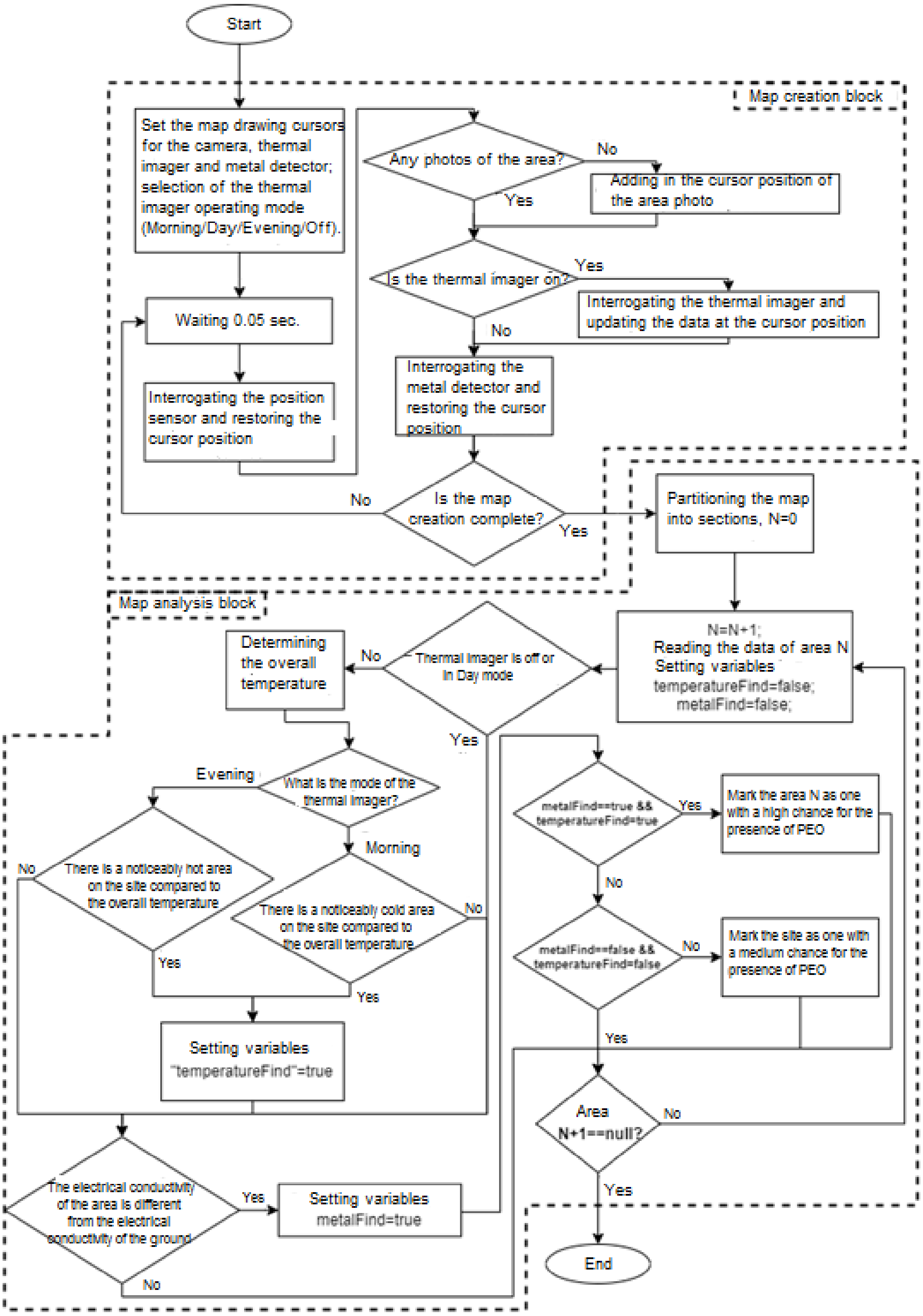


Fig. 3. Algorithm of the software control system of identification of potentially explosive objects in open areas

Accuracy – the idea of finding or not finding a potentially explosive object in a certain area consists of the result of the two most common methods of detecting potentially explosive objects at once.

Wide range of objects, determined by the fact that the system can detect all objects that can be detected separately by thermal imager and metal detector.

The disadvantages of the system is the speed and reduced accuracy or inability to explore the area at a certain time of day or weather conditions.

Speed is a disadvantage because due to the increased accuracy and the use of two methods at the same time, it takes time to complete a full route.

Reduced accuracy or inability to survey an area at certain times of day or weather conditions is due to the use of a thermal imager, less effective in certain times of day and territorial conditions. In addition, using a drone under certain weather conditions can decrease accuracy, but this is corrected by using more advanced drone stabilization systems and design solutions.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Further research to improve the system could add an automatic drone control system, such as a control system using a dedicated coordinator station, which would allow positioning and control of the drone with centimeter accuracy.

References

1. Barbashyn, V. V. Smyrnov, O. M. and Tolkunov, I. O. (2015), *Utilization and destruction of explosive objects. Study guide (in three volumes). Volume I. Procedure and rules for disposal of explosive objects* [*Utylizatsiia ta znyshchennia vybukhonebezpechnykh predmetiv. Navchalnyi posibnyk (v trokh tomakh). Tom I. Poriadok ta pravyla utylizatsii vybukhonebezpechnykh predmetiv*], NUTsZU, Kharkiv, 416p.
2. Smirnov, O. M., Barbashyn, V. V., Tolkunov, I. O. (2015), *Utilization and destruction of explosive objects. Study guide (in three volumes). Volume 2. Safety measures when handling missiles and ammunition during disposal operations* [*Utylizatsiia ta znyshchennia vybukhonebezpechnykh predmetiv. Navchalnyi posibnyk (v trokh tomakh). Tom 2. Zakhody bezpeky pry povodzhenni z raketamy i boieprypasamy pid chas provedennia robit z utylizatsii"*], NUTsZU, Kharkiv,484 p.
3. Pizing, M., "How mines are detected and neutralized" ["Yak vyiavliaiut i zneshkodzhuiut miny"], available at: https://www.bbc.com/ukrainian/vert-fut-39698204 (last accessed: 18.05.2022).
4. Bevs, A. M., Tolkunov, I. O. (2018), "State management of humanitarian demining processes in Ukraine" ["Derzhavne upravlinnia protsesamy humanitarnoho rozminuvannia v Ukraini"], *Materials of the All-Ukrainian scientific and practical conference State management in the field of civil protection: science, education, practice*, P. 154 –158.
5. Hovdun, A. V., Polotai, O. I. (2017), "Humanitari and emining projects and their features" ["Proekty humanitarnoho rozminuvannia ta yikh osoblyvosti"], *Collection of scientific works of LSU BZD Problems and prospects of development of life safety system*, No. 2, P. 95.
6. Tymyshyn, O. Y.(2019), "Innovative technologies in working with explosive objects" ["Innovatsiini tekhnolohii u roboti z vybukhonebezpechnymy obiektamy"], *Development of science and technology: problems and prospects: collection of theses of the round table on the occasion of the celebration of Science Day - 2019 in Ukraine*, P. 169−172.
7. "Products of telerob", available at: https://www.telerob.com/de/ (last accessed: 20.05.2022).
8. "The robots being used by police to help capture criminals", available at: https://www.news.com.au/technology/gadgets/mobile-phones/the-robots-being-usedby-police-to-help-capture-criminals/news-story/69c0358276a548cf0d6a65224eff647f (last accessed: 22.05.2022).
9. Yakovlev, O. V., Parfilo, O. A. (2017), "Analysis of the experience of using forensic equipment during the inspection of the scene in the event of the discovery of an improvised explosive device" ["Analiz dosvidu vykorystannia kryminalistychnoi tekhniky pry ohliadi mistsia podii u razi vyiavlennia samorobnohov ybukhovoho prystroiu"], Forensics and forensic examination, No. 62, P. 138−145.
10. Alqudsi, Y. S., Alsharafi, A. S., Mohamed, A. (2021), "A Review of Airborne Landmine Detection Technologies: Unmanned Aerial Vehicle-Based Approach", *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, P. 1–5. **DOI:** https://doi.org/10.1109/icoten52080.2021.9493528
11. Fardoulis, J., Depreytere, X., Gallien, P., Djouhri, K., Abdourhmane, B., Sauvage, E. (2020), "Proof: How Small Drones Can Find Buried Landmines in the Desert Using Airborne IR Thermography", *The Journal of Conventional Weapons Destruction*, No. 24 (2), P. 15. **DOI:** https://doi.org/10.5281/zenodo.4409641
12. Barbedo, J. (2019), "A Review on the Use of Unmanned Aerial Vehicles and Imaging Sensors for Monitoring and Assessing Plant Stresses", *Drones*, No. 3 (2), P. 40. **DOI:** https://doi.org/10.3390/drones3020040
13. Mogili, U. R., Deepak, B. B. V. L. (2018), "Review on Application of Drone Systems in Precision Agriculture", *Procedia Computer Science*, No.133, P. 502–509. **DOI:** https://doi.org/10.1016/j.procs.2018.07.063
14. Huang, H., Savkin, A.V. (2018), "Towards the Internet of Flying Robots: A Survey", *Sensors*, No. 18 (11), P. 4038. **DOI:** https://doi.org/10.3390/s18114038
15. "Alexander Graham Bell's 5 most important inventions" available at: https://uk.warbletoncouncil.org/inventos-alexander-graham-bell-6411 (lastaccessed: 19.05.2022).
16. Colorado, J., Perez, M., Mondragon, I., Mendez, D., Parra, C., Devia, C., Martinez-Moritz, J., Neira, L. (2017), "An integrated aerial system for landmine detection: SDR-based Ground Penetrating Radar on board an autonomous drone", *AdvancedRobotics*, No. 31 (15), P.791–808. **DOI:** https://doi.org/10.1080/01691864.2017.1351393
17. Yoo, L. S., Lee, J. H., Lee, Y. K., Jung, S. K., Choi,Y. (2021), "Application of a Drone Magnetometer System to Military Mine Detection in the Demilitarized Zone", Sensors, No. 21 (9), P. 3175.**DOI:** https://doi.org/10.3390/s21093175

Received 29.06.2022

Відомості про авторів / Сведения об авторах / About the Authors

Пахниць Іван – студент кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки, Харківський національний університет радіоелектроніки, Харків, Україна; e-mail: ivan.pakhnyts@nure.ua; ORCID ID: https://orcid.org/0000-0002-3112-7042.

Пахниц Иван – студент кафедры компьютерно-интегрированных технологий, автоматизации и мехатроники, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

Pakhnyts Ivan –student of the Department of Computer-Integrated Technologies, Automation and Mechatronics, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

Хрустальова Софія Володимирівa– кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки,Харків, Україна; e-mail: sofiia.khrustalova@nure.ua; ORCID ID: https://orcid.org/0000-0003-3363-4547.

Хрусталева София Владимировна – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

Khrustalova Sofiia – PhD (EngineeringSciences), Docent, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

Хрустальов Кирило Львович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, Харків, Україна; e-mail: kirill.khrustalev@nure.ua; ORCID ID: https://orcid.org/0000-0002-0687-5153.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2022. No. 2 (20)

Хрусталев Кирилл Львович – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

Khrustalev Kirill – PhD (EngineeringSciences), Docent, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

СИСТЕМА ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОТЕНЦІЙНО ВИБУХОНЕБЕЗПЕЧНИХ ОБ'ЄКТІВ НА ВІДКРИТІЙ МІСЦЕВОСТІ

Предметом даного дослідження є методи, засоби та системи виявлення потенційно небезпечних об’єктів воєнного призначення на відкритій місцевості. **Метою** дослідження є розроблення системи виявлення та ідентифікації потенційно вибухонебезпечних об’єктів воєнного призначення з використанням безпілотного літаючого апарату (дрону), який налічує в своєму складі систему виявлення вибухонебезпечного предмету за допомогою металодетектора з технологією корегуванням висоти польоту та методу виявлення за допомогою тепловізора. Для досягнення мети вирішені такі **завдання:** проведено огляд та аналіз сучасних методів засобів та систем виявлення та ідентифікації потенційно вибухонебезпечних об’єктів воєнного призначення, визначено класифікацію вибухонебезпечних об’єктів, що ідентифікуються, обрано компоненти системи, розроблено структурну схему та алгоритм роботи програмного засобу управління системою ідентифікації потенційно вибухонебезпечних об’єктів на відкритій місцевості, створено програмний засіб виявлення та ідентифікації потенційно вибухонебезпечних об’єктів на відкритій місцевості. В роботі використовуються наступні **методи:** математичний метод побудови картографічних сіток, метод реєстрації інфрачервоного випромінювання, метод вихрових струмів, методи та засоби збору та обробки даних. Отримано наступні **результати:** обрано компоненти системи, розроблено структуру схему та алгоритм роботи програмного засобу управління системою ідентифікації потенційно вибухонебезпечних об’єктів на відкритій місцевості, створено відповідне програмне забезпечення. **Висновки:** застосування запропонованої системи дозволяє підвищити точність знаходження або відсутність потенційно вибухонебезпечного об’єкту у певній ділянці за рахунок використання одразу двох методів виявлення потенційно вибухонебезпечних об’єктів, надає можливість ідентифікувати достатньо широкий спектр об’єктів. Система, що розроблена є безпечною, оскільки керується оператором, який знаходиться на безпечній відстані, дозволяє отримати спеціальні мапи з позначками місцевості з інформацією про можливу наявність потенційно вибухонебезпечних об’єктів на певних ділянках місцевості та загалом мапи сигналів металошукача та тепловізора.

Ключові слова: вибухонебезпечний об'єкт; міна; система виявлення та ідентифікації; дрон; тепловізор; металодетектор.

СИСТЕМА ВЫЯВЛЕНИЯ И ИДЕНТИФИКАЦИИ ПОТЕНЦИАЛЬНО ВЗРЫВООПАСНЫХ ОБЪЕКТОВ НА ОТКРЫТОЙ МЕСТНОСТИ

Предметом данного исследования являются методы, средства и системы выявления потенциально опасных объектов военного назначения на открытой местности. **Целью** исследования является разработка системы выявления и идентификации потенциально взрывоопасных объектов военного назначения с использованием беспилотного летающего аппарата (дрона), который содержит в своем составе систему обнаружения взрывоопасного предмета с помощью металлодетектора с технологией коррекции высоты полета и метода обнаружения с помощью тепловизора. Для достижения цели решены следующие **задачи**: проведен обзор и анализ современных методов, средств, систем выявления и идентификации потенциально взрывоопасных объектов военного назначения, определена классификация идентифицируемых взрывоопасных объектов, выбраны компоненты системы, разработана структурная схема и алгоритм работы программного средства управления системой идентификации потенциально взрывоопасных объектов на открытой местности, создано программное средство выявления и идентификации потенциально взрывоопасных объектов на открытой местности. В работе используются следующие **методы**: математический метод построения картографических сетей, метод регистрации инфракрасного излучения, метод вихревых токов, методы и средства сбора и обработки данных. Получены следующие **результаты:** выбраны компоненты системы, разработана структура схемы и алгоритм работы программного средства управления на открытой местности, создано соответствующее программное обеспечение. **Выводы**: применение предлагаемой системы позволяет повысить точность нахождения или отсутствие потенциально взрывоопасного объекта на определенном участке за счет использования сразу двух методов обнаружения потенциально взрывоопасных объектов, дает возможность идентифицировать достаточно широкий спектр объектов. Разработанная система является безопасной, поскольку управляется оператором, который находится на безопасном расстоянии, позволяет получить специальные карты с пометками местности и информацией о возможном наличии потенциально взрывоопасных объектов на определенных участках местности и в целом карты сигналов металлоискателя и тепловизора.

Ключевые слова: взрывоопасный объект; мина; система выявления и идентификации; дрон; тепловизор; металлодетектор.

Бібліографічні описи / Bibliographic descriptions

Пахниць І., Хрустальова С. В., Хрустальов К. Л. Система виявлення та ідентифікації потенційно вибухонебезпечних об'єктів на відкритій місцевості. *Сучасний стан наукових досліджень та технологій в промисловості*. 2022. № 2 (20). С. 106–112. DOI: https://doi.org/10.30837/ITSSI.2022.20.106

Pakhnyts, I., Khrustalova, S., Khrustalev, K. (2022), "System for detection and identification of potentially explosive objects in open area", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (20), P. 106–112. DOI: https://doi.org/10.30837/ITSSI.2022.20.106

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2022. № 2 (20) ISSN 2524-2296 (online)

АЛФАВІТНИЙ ПОКАЖЧИК **ALPHABETICAL INDEX**

НАУКОВЕ ВИДАННЯ

СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ

Щоквартальний науковий журнал

№ 1 (19), 2022

Відповідальний секретар журналу *І. Г. Перова*
Відповідальний за випуск *А. А. Коваленко*
Комп'ютерна верстка *А. І. Коломієць*

АДРЕСА РЕДАКЦІЇ:
Україна, 61166, м. Харків, проспект Науки, 14
Тел.: +38 (057) 704-10-51
Веб-сайт: http://itssi-journal.com
E-mail: journal.itssi@gmail.com

Формат 60×84/8. Умов. друк. арк. 11,25. Тираж 150 прим.

Віддруковано з готових оригінал-макетів в типографії ФОП Андреєв К.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис №24800170000045020 від 30.05.2003.

61166, Харків, вул. Серпова, 4, тел. 063-993-62-73
e-mail: ep.zakaz@gmail.com