МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 13, № 3-4

Volume 13, No. 3-4

Одеса – 2023
Odesa – 2023

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odesa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Національного університету «Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: 1 Шевченка пр., Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odesa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

ЗМІСТ/CONTENTS

DOI 10.15276/imms.v13.no3-4.195
UDC 004.93'11:004.942

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 195-203

USE OF PRE-TRAINED NEURAL NETWORKS FOR MODELING NONLINEAR DYNAMIC OBJECTS

A.A. Orlov

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: andrey.orlov.od@gmail.com

The paper considers a class of problems of identification of nonlinear dynamic objects with continuous characteristics using neural networks with time delays. The multiple use of pre-trained neural networks to identify objects of different nature with similar laws of functioning is substantiated. The aim of this work is to reduce the training time of neural network models without significant loss of accuracy by developing a method for pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics. The scientific novelty of the work is the further development of the method of pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics, which allows reducing the training time of neural network models without significant loss of accuracy. The method consists in extracting general patterns from the base dataset at the pre-training stage and using them to solve specific problems at the stage of retraining models on the target dataset. A formal criterion is proposed to determine the moment of termination of the neural network pre-training, the use of which allows avoiding retraining of the base model and ensuring a significant reduction in the model training time on the target dataset. The practical significance of the work is to develop an algorithm for the method of pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics, which reduces the training time of neural network models and the loss of model accuracy. To study the convergence rate of the training algorithm and modeling accuracy, an experiment was conducted with test nonlinear dynamic objects. The obtained modeling results demonstrate the effectiveness of the proposed method. The value of this study is *to* determine the area of effective use of the proposed method, namely, when the general and target datasets do not have significant differences and the target dataset is of sufficient size to reflect the properties of the research object.
Keywords: nonlinear dynamic objects, modeling, neural networks with time delays, pre-training.

Introduction. In the modern world, against the background of rapid technological development, the issues of effective modeling of modern management objects are becoming increasingly relevant. Classical methods, although reliable and widely used, are increasingly proving to be insufficiently effective for representing complex objects of the world [1, 2]. Complex control objects are characterized by a high degree of nonlinearity and dynamics, the ability to adapt to various environmental conditions and operating requirements.

Due to the above requirements, researchers and engineers prefer to consider complex objects as a "black box" whose internal structure and functioning algorithms are not accessible to an external observer [1, 3]. Such objects are well described by simulation models that approximate or mimic the behavior of a real system, which is difficult or impossible to express analytically. Simulation models are built on the basis of an input/output experiment, in which an object is analyzed based on its response (output signals) to external influences (input signals).

Today, neural networks are widely used as simulation models [2]. In the world of rapidly evolving technologies, neural networks have become an essential tool in the field

of artificial intelligence, demonstrating impressive capabilities in solving complex tasks ranging from pattern recognition and natural language synthesis to identifying simulation models.

Such models can be trained to simulate complex behavior based on the observation of input and output data, which is why they are often used to model time dependencies and predict the behavior of complex dynamic systems.

Despite advances in the field of neural networks, the problems of effective learning with limited data and computational limitations remain unresolved [4]. Therefore, the task of developing methods to improve the characteristics of neural networks remains relevant.

Analysis of research and publications. Different approaches are used to overcome the limitations that hinder the development of neural networks in the field of complex object identification, depending on the application, object properties, availability and amount of training data. Having systematized the research in the field of improving neural network training methods, the following key areas can be identified.

Improvement of learning methods aimed at creating models capable of accelerating learning and quickly adapting to new tasks based on limited data. This area includes experiments with activation functions [5], learning methods [4], and the structure of neural networks [6].

The development of learning methods includes adaptive optimization algorithms such as Adafactor, LAMB, Ranger [7], which can more effectively use gradients for learning, as well as techniques for thinning layers and parameters in neural networks, which help reduce the number of calculations and speed up the learning process. This approach is implemented using the Sparse Training and Magnitude Pruning methods [8].

The choice of network architecture is carried out using automatic machine learning (AutoML) methods, which significantly speeds up the model development process. Such methods include Neural Architecture Search (NAS) [6, 9].

The construction of surrogate models makes it possible to reduce the size of neural network models and speed up computations without significant loss of accuracy, which is especially relevant given the growing demands on computing resources and the use of neural networks on mobile devices. This area includes such algorithms as Deep Compression [10], the construction of linear [3] and integral [11] surrogate models.

Pre-training allows neural networks to extract information from large amounts of data before the main training phase and can accelerate model convergence during training on target data, increasing their performance even on datasets of limited size [12].

A variation of pre-training is the transfer learning technique, which allows using the knowledge gained from solving one problem to improve the solution of another [13]. This approach is actively used when the available training data for a new task is limited, and it can significantly speed up learning and improve the generalizability of the model.

Modeling practice is well known for cases when you have to solve similar tasks that are repeated in different fields of activity due to the fact that objects of different nature have similar laws of functioning. In the field of software development, such tasks have long been successfully solved by reusing once-written code in the form of function libraries, classes, or a framework, depending on the degree of generalization of the task.

In the emerging field of simulation modeling, this approach is just beginning to be used. In this case, a pre-trained neural network can be used as a reusable solution. In this case, the construction of the target model consists of extracting general patterns from the base dataset at the pre-training stage and using them to solve specific problems at the stage of training models on the target dataset [12].

The described technique has several advantages. First, it allows using large amounts of data to extract general patterns, which is especially useful in the absence of sufficient data in the target dataset. Secondly, pre-trained models can be successfully applied to different tasks, even if they are related to different areas. This saves time and resources,

as there is no need to train the model from scratch for each new task. Thus, thanks to pre-training, neural networks are able to demonstrate impressive results even in conditions of limited resources.

This approach is a fairly common and effective practice for reducing the training time of convolutional neural networks and building universal models before they are retrained on a specific task. VGG (Visual Geometry Group) pre-trained convolutional networks are widely known and have been successfully used for image classification tasks, GPTs are designed for text generation.

At the same time, there is a lack of work in the field of pre-training neural networks that model the behavior of nonlinear dynamic objects with continuous characteristics.

This article discusses methods of improving the characteristics of neural networks based on the idea of pre-training as a promising direction of identification of complex continuous objects, which is dynamically developing and able to effectively cope with the requirements of modern modeling tasks.

The aim of this work is to reduce the training time of neural network models without significant loss of accuracy by developing a method for pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics.

Formulation of the research problem. The formal statement of the problem of pre-training neural networks can be formulated as follows.

Let S be an initial problem for which there is a large amount of labeled data (dataset D_S):

$$D_S = \{(x_i^S, y_i^S)\}, \quad (1)$$

where x_i^S – is the input data, y_i^S – is the corresponding output data (labels) of the dataset D_S, $i=1,...,N_S$, N_S – is the size of the dataset D_S.

Let us denote the basic model as a neural network trained on the data of the problem S with parameters θ_S as $f_{\theta S}$.

Let T be a target task for which there is a limited amount of labeled data (dataset D_T):

$$D_T = \{(x_j^T, y_j^T)\}, \quad (2)$$

where x_j^T – is the input data, y_j^T – is the corresponding output data (labels) of the dataset D_T, $j=1,...,N_T$, N_T is the size of the dataset D_T.

At the same time, using the parameters θ_S of the base model $f_{\theta S}$ to initialize the weights of the target model $f_{\theta T}$, it is possible to train the target model $f_{\theta T}$ on the data of the dataset D_T to adapt it to the target task.

A model $f_{\theta S}$ is called a pre-trained model if the minimum loss function is ensured for the target model $f_{\theta T}$ trained on the basis of parameters θ_S:

$$\theta_T^* = arg\ min_{\theta T} L_T(f_{\theta T}(x_j^T), y_j^T), \quad (3)$$

where L_T – is the loss function adopted for the target problem.

At the same time, to assess the quality of the pre-trained model $f_{\theta S}$ (measuring the success of the base model), we can introduce the concept of performance $P_{\theta T}$ of the model $f_{\theta S}$ on the target dataset D_T as a metric that characterizes the model's ability to solve the target problem:

$$P_{\theta T} = E_{\theta T} / t_{\theta T}, \quad (4)$$

where $E_{\theta T}$ – is the difference between the predicted $f_{\theta T}(x_j^T)$ and the true y_j^T values of the objective function; $t_{\theta T}$ – is the time spent on training the model with an accuracy of $E_{\theta T}$.

In practice, the mean absolute error *mae*, mean squared error *mse,* or coefficient of determination *R-squared can be* used as $E_{\theta T}$. The number of epochs of model training can be used as $t_{\theta T}$. Calculating the model performance allows you to assess how well the pre-trained model fits a specific target task and data.

The main part. The basic idea of pre-training is that a neural network is first trained to extract general features and patterns from data that can be applied to different tasks. This pre-trained model is then retrained on a narrower sample of data related to a specific task.

However, when implementing this method, the problem arises of finding the moment when pre-training stops, when the model is already able to extract general patterns from the underlying dataset and, at the same time, has not adapted to the data of a particular task, i.e., the neural network has not been retrained. Violation of this balance causes the following problems.

1. Early termination of pre-training (undertraining): if the pre-trained and target models differ significantly, the retraining process may take longer and be less effective.

2. Late termination of pre-training (retraining): if the pre-trained model has adapted to the data of the base dataset, then the problem of Domain Shift arises. This can lead to a loss of model performance on the target task due to the mismatch between the characteristics of the base and target datasets.

The developed method of pre-training neural networks should take into account both limitations by determining the pre-training threshold, which reduces the time of model training while ensuring a given accuracy.

A time-delay neural network (TDNN) is used as a neural network model of nonlinear dynamic objects with continuous characteristics. Due to their simplicity and versatility, TDNNs have become the most widespread. The most commonly used TDNN structure consists of three layers: input, hidden, and output [14].

In this structure, the input layer of a TDNN includes M neurons – the memory length of the object model. The number of neurons M choses to best reflect the dynamic properties of the object. The hidden layer includes K neurons with a nonlinear activation function. The number of neurons K choses to best reflect the nonlinear properties of the object. The output layer of TDNN contains 1 neuron with a linear activation function.

The input layer receives data

$$\mathbf{x}(t_n)=[x(t_n), x(t_{n-1}), \ldots, x(t_{n-M-1})],\ t_n = n\Delta t,\ n=1, 2, \ldots \quad (5)$$

The signal $y(t_n)$ at the output layer at time t_n depends on the values of the input signal $\mathbf{x}(t_n)$ and is determined by the expression [14]:

$$y(t_n) = b_0 + S_0 \sum_{i=1}^{K} w_i S_i \left(b_i + \sum_{j=1}^{M} w_{i,j} x(t_{n-j}) \right) \quad (6)$$

where b_0, b_i – are the biases of the neurons of the output and hidden layers, respectively; S_0, S_i – are the activation functions of the neurons of the output and hidden layers, respectively; w_i, $w_{i,j}$ – are the weighting coefficients of the neurons of the output and hidden layers, respectively.

Taking into account the well-known fact that in multilayer neural networks the first layer identifies the most general features, and the subsequent layers identify more specific features, the following method of pre-training neural networks with time delays is proposed in this paper for identifying nonlinear dynamic objects with continuous characteristics.

Stage 1. The neural network model f_S is trained on the data of the basic dataset $\{(\mathbf{x}_S(t_n), y_S(t_n))\}$. In this case, the criterion for stopping the training process is the simultaneous fulfillment of the following conditions: the standard deviation of the parameters of the input layer of the network at epochs $k+1$ and k does not exceed a predetermined value E_1 and the standard deviation of the parameters of the hidden layer of the network at epochs $k+1$ and k *is* not less than a predetermined value E_2:

$$\begin{cases} e_1 = \dfrac{1}{KM}\sum\limits_{i=1}^{K}\sum\limits_{j=1}^{M}\left(w_{i,j}^{k+1} - w_{i,j}^{k+1}\right)^2 \le E_1 \\ e_2 = \dfrac{1}{K}\sum\limits_{i=1}^{K}\left(w_i^{k+1} - w_i^{k+1}\right)^2 \ge E_2 \end{cases} \quad (7)$$

Stage 2. The neural network model $y_T(t_n)$ is trained on the data of the target dataset $\mathbf{x}_T(t_n)$. The parameters of the base model $y_S(t_n)$ are used as the initial state of the target model $y_T(t_n)$. In the process of training the target model, the pre-trained weights of the neural network are not fixed in order to correct and adjust them to the data of the target task during further training. This process is called fine-tuning.

The criterion for stopping the learning process is the absolute deviation of the model output from the target values.

The proposed method of pre-training neural networks with time delays for the identification of nonlinear dynamic objects is tested on the task of identifying a test object with continuous characteristics.

Experimental setup. The accuracy of TDNNs and the time of their construction using pre-training of neural network models is studied on the example of a basic dataset. The dataset is formed from a set of input signals $x(t)=a\Theta(t)$ in the form of step functions with different amplitudes a and their corresponding output signals $y(t)=f(x(t))$.

In [15], it was established that TDNN models are not invariant to the shape of the input signal and can adequately reflect the properties of a dynamic object when trained on a sufficient amount of input and output signals of the same type as in the test data set. Therefore, the common nonlinear and dynamic links shown in Table 1 are used as a black box transducer f.

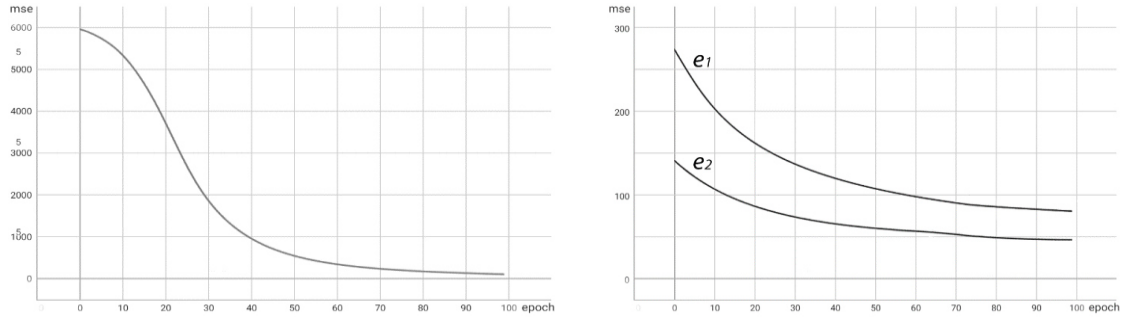
Table 1

Nonlinear and dynamic functions that form the basic dataset

№	Title	Expression
1	Inertia-free amplifier	$y(t)=Rx(t)$
2	Integrator	$y(t)=1/T\int_0^t x(t)d(t)$
3	Inertial link	$Tdy(t)/dt+ y(t) = x(t)$
4	Oscillating link	$c\ d_1{}^2\ y(t)/dt^2 + c_2\ dy(t)/dt + c_3\ y(t)= x(t)$
5	The lagging link	$y(t)=Kx(t-\tau),\ t>\tau$

A three-layer neural network with time delays is used as a pre-trained neural network model. In this structure, the input and hidden layers of the network have $M=K=50$ neurons with activation in the form of a linear rectifier [15]. The output layer of the TDNN includes 1 neuron with a linear activation function. This structure of the neural network ensures the level of losses set by the experimental conditions ($mse < 50$) with an acceptable training time ($epochs < 100$). The resulting TDNN was used to study the accuracy of models of dynamic objects with smooth and significant nonlinearities.

The process of preliminary training of the described model on the data of the basic dataset is demonstrated in Fig. 1: a plot of the loss function versus the number of training epochs (Fig. *1a)* and a plot of the model training accuracy metric versus the number of training epochs (Fig. *1b)*.



a *b*

Fig. 1. TDNN model training process on the base dataset: *a* – graph of the loss function versus the number of training epochs; *b* – graph of the model training accuracy metric versus the number of training epochs.

Taking into account the stopping conditions (7), the pre-learning process stops after the end of epoch **7**.

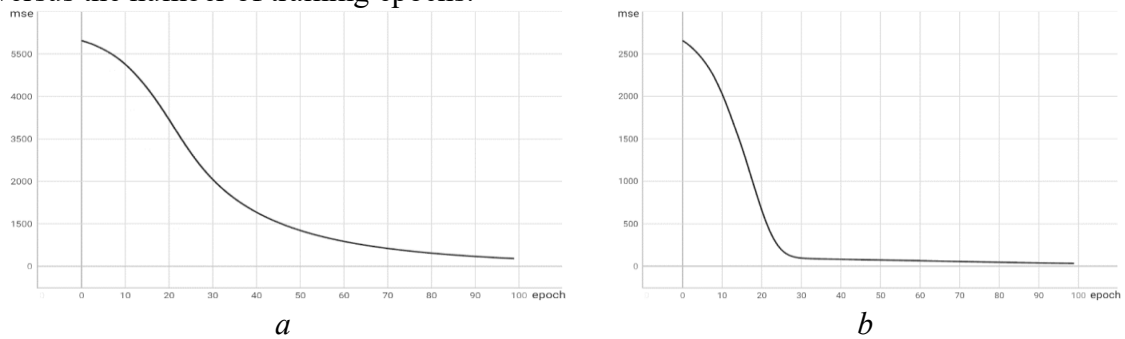
We study the accuracy of TDNNs and the time of their construction at the stage of target training using the example of a target dataset. The dataset is formed from a set of input signals $x(t)=a\Theta(t)$ in the form of step functions with different amplitudes a ($a\in(0,1)$) and the corresponding output signals [14] in the form of a linear function with saturation:

$$y(t)=\begin{cases} s, x(t) > p \\ gx(t), x(t) \le p \end{cases} \quad (8)$$

where s – is the saturation level, p is the saturation point, and g is the gain.

The process of training a TDNN model with randomly selected weights on the target dataset is shown in Fig. 2*a*: a graph of the model training accuracy metric versus the number of training epochs.

The process of training a TDNN model by retraining a pre-trained model on the target dataset is demonstrated in Fig. 2*b*: a plot of the model training accuracy metric versus the number of training epochs.



a *b*

Fig. 2. Graph of the model training accuracy metric versus the number of training epochs on the target dataset: *a* – models with randomly selected weights; *b* – by retraining a pre-trained model.

Fig. 2 shows a 3.7-fold reduction in the time required to train the TDNN model on the target dataset compared to the full training procedure, while ensuring comparable accuracy of both models.

To investigate the modeling accuracy, the resulting neural network is verified on a test nonlinear dynamic object given in [15]. In Fig. 3 shows a comparison of the output signals $y_n(t)$, $y_v(t)$ and $y(t)$, obtained as a result of the action of the step signal $x(t)=a\Theta(t)$ (a=0.65) at the inputs of the TDNN model, the second-order integral-step series [14] (chosen as a method of deterministic identification for comparison), and the simulation

model of the test nonlinear dynamic object, respectively. The graph shows a 15% advantage in accuracy of the proposed TDNN model over the integral-step model.

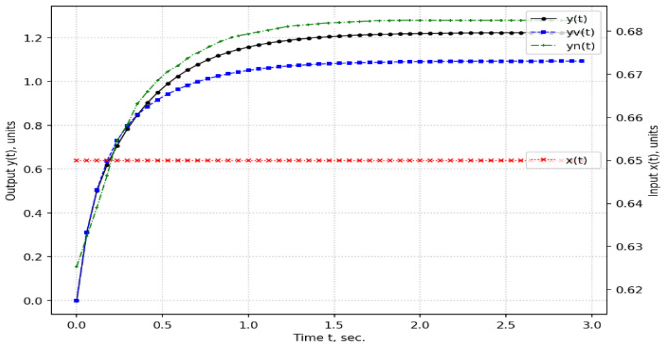


Fig. 3. Comparison of the output signals yn(t), yv(t) and y(t), obtained as a result of the action of the signal x(t)=aΘ(t) on the inputs of the TDNN model, the integro-power series and the simulation model of a nonlinear dynamic object, respectively .

Discussion of results. The obtained simulation results show that the use of TDNN models with pre-training to identify nonlinear dynamic objects with continuous characteristics can significantly reduce the training time of neural network models without losing accuracy. However, this method is demanding to meet the following conditions:

Task Mismatch: if the tasks for which the model has been trained and the target task differ significantly, the trained model may be less effective. A special case is the Domain Shift problem, where a pre-trained model is trained on data that is significantly different in distribution from your target data.

Insufficient Data for Fine-Tuning: if there is a limited amount of labeled data for the target task, then retraining a trained model may face the problem of overtraining or undertraining.

Model Size: some pre-trained models can be large and require large computing resources to run and retrain.

Thus, the area of effective application of the method of pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics is when the general and target datasets do not have significant differences and the target dataset is of sufficient size to reflect the properties

Conclusions. In this paper, an attempt has been made to further develop the method of pre-training neural networks with time delays in the tasks of identifying nonlinear dynamic objects with continuous characteristics in order to reduce the training time of neural network models without significant loss of accuracy.

The novelty of the proposed method lies in the use of a formal criterion for determining the moment of termination of pre-training, which allows avoiding retraining of the base model and providing a significant reduction in the model training time on the target dataset.

The proposed method of pre-training neural networks with time delays for the identification of nonlinear dynamic objects is tested, which demonstrated a 3.7-fold reduction in model training time on the target dataset compared to the full training procedure while ensuring comparable accuracy of both models.

The advantages of pre-training include the ability to improve model performance when there is a lack of labeled data for the target task. This is especially useful in situations where the collection of labeled data requires a lot of effort and the base task has an excess of data. The area of effective use of the proposed method is highlighted.

References

1. Rudin C., Radin J. Why are we using black box models in AI when we don't need to? A lesson from an explainable AI competition. *Harvard Data Science Review*. 2019. V.2. No. 1.
2. Mitrea C.A., Lee C.K.M., Wu Z. A comparison between neural networks and traditional forecasting methods: A case study. *International journal of engineering business management*. 2009. V.1. No. 2. P. 19-24.
3. Karim R., Shajalal, Grass A. Interpreting Black-box Machine Learning Models for High Dimensional Datasets. *arXiv preprint*. 2022. URL: arxiv.org/abs/2208.13405.
4. Sen J. Machine Learning - Algorithms, Models and Applications. London, UK: IntechOpen, 2021.
5. Sharma S., Sharma S., Athaiya A. Activation functions in neural networks. International *Journal of Engineering Applied Sciences and Technology*. 2020. V.4, No 12. P. 310-316.
6. Karampiperis P., Manouselis N., Trafalis T.B. Architecture selection for neural networks. *Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02*, *Honolulu, HI, USA*. 2002. V.2. P. 1115-1119.
7. Pasechnyuk D., Prazdnichnykh A., Evtikhiev M., Bryksin T. Judging Adam: Studying the Performance of Optimization Methods on ML4SE Tasks. *arXiv:2303.03540*
8. Hoefler T., Alistarh D., TalBen-Nun N.D., Peste A. Sparsity in Deep Learning: Pruning and growth for efficient inference and training in neural networks. *Journal of Machine Learning Research.* 2021. No 23. P.1-124.
9. Elsken T., Metzen J.H., Hutter F. Neural Architecture Search. In: Automated Machine Learning. The Springer Series on Challenges in Machine Learning. Cham: Springer, 2019. 223 p.
10. Li Z., Li H., Meng L. Model Compression for Deep Neural Networks: A Survey. *Computers.* 2023. No. 12. P.60.
11. Krykun V. Improving the accuracy of the neural network models interpretation of nonlinear dynamic objects. *Mathematical and computer modeling. Series: Technical sciences*. 2022. No. 23. P. 31-41.
12. Lu Y., Jiang X., Fang Y., Shi Ch. Learning to Pre-train Graph Neural Networks. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2021. V.33. No.5. 10p.
13. Hosna A., Merry E., Gyalmo J. Transfer learning: a friendly introduction. *J Big Data.* 2022. No. *9*. V.102.
14. Fomin O., Polozhaenko S., Krykun V., Orlov A., Lys D. Interpretation of Dynamic Models Based on Neural Networks in the Form of Integral-Power. *Lecture Notes in Networks and Systems*. 2022. V. 536. P. 258-265.
15. Fomin O., Speranskyy V., Krykun V., Tataryn O., Litynskyi V. Models of dynamic objects with significant nonlinearity based on time-delay neural networks. *Bulletin of Cherkasy State Technological University. Technical sciences.* 2023. No. 3. P. 97–112.

ВИКОРИСТАННЯ ПЕРЕДНАВЧЕНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ МОДЕЛЮВАННЯ НЕЛІНІЙНИХ ДИНАМІЧНИХ ОБ'ЄКТІВ

А.А. Орлов

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: andrey.orlov.od@gmail.com

Розглянуто клас задач ідентифікації нелінійних динамічних об'єктів із безперервними характеристиками за допомогою нейронних мереж із часовими затримками. Обґрунтовано багаторазове використання попередньо навчених нейронних мереж для ідентифікації об'єктів різної природи, що мають схожі закони функціонування. Метою роботи є скорочення часу навчання нейромережевих моделей без значної втрати точності шляхом розвитку методу попереднього навчання нейронних мереж із часовими затримками в задачах ідентифікації нелінійних динамічних об'єктів із безперервними характеристиками. Наукова новизна роботи полягає у подальшого розвитку метод попереднього навчання нейронних мереж із часовими затримками в задачах ідентифікації нелінійних динамічних об'єктів з безперервними характеристиками, що дозволяє скоротити час навчання нейромережевих моделей без значної втрати точності. Метод полягає у вилученні загальних закономірностей із базового датасету на етапі попереднього навчання та використанні їх для розв'язання конкретних задач на етапі донавчання моделей на цільовому датасеті. Для визначення моменту припинення попереднього навчання нейронної мережі запропоновано формальний критерій, використання якого дає змогу уникнути перенавчання базової моделі та забезпечити суттєве скорочення часу навчання моделі на цільовому датасеті. Практичне значення роботи полягає в розробці алгоритму методу попереднього навчання нейронних мереж із часовими затримками в задачах ідентифікації нелінійних динамічних об'єктів з безперервними характеристиками, що дозволяє скоротити час навчання нейромережевих моделей втрати точності моделі. Дослідження швидкості збіжності алгоритму навчання та точності моделювання проведено експеримент з тестовими нелінійними динамічними об’єктами. Отримані результати моделювання свідчать про ефективність запропонованого методу. Цінність проведеного дослідження полягає у визначенні області ефективного використання запропонованого методу, а саме коли загальний та цільовий датасети не мають суттєвих розбіжностей та цільовий датасет має достатній розмір для відображення властивостей об’єкту дослідження.

Ключові слова: нелінійні динамічні об'єкти, моделювання, нейронні мережі з часовими затримками, переднавчання.

DOI 10.15276/imms.v13.no3-4.204
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 204-211

THE ALGORITHM FOR ENCRYPTION OF GRAPHIC INFORMATION BASED ON CHAOTIC MAP AND GALOIS FIELD TRANSFORM

O.O. Palagin, A.V. Sokolov

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: radiosquid@gmail.com

The current stage of development of information technologies is characterized by a significant increase in the use of graphic data, i.e., digital video and digital images combined with the widespread use of resource-constrained platforms, such as IoT and IoBT devices, mobile devices, as well as embedded devices. These circumstances condition the importance of the development of algorithms for encrypting graphic information, which would ensure high security for the least number of computational operations. Today, dynamic chaos theory is most often used for the development of such cryptographic algorithms. However, the optimal structure of the cryptographic algorithm for image encryption has not yet been found. In this paper, we propose a combination of the advantages of traditional SP networks and a gamma generator based on a Hyper-Chaotic Modified Robust Logistic Map to build an effective image encryption algorithm, capable of providing a high level of security. The proposed cryptographic algorithm uses high-quality S-boxes based on the Galois field transform, as well as P-boxes based on permutations generated using the Nyberg construction, while segmentation and further processing of three-dimensional image blocks are used, which allows for an increase in the diffusion effect. Numerous tests of the stochastic quality of cryptograms obtained using the developed cryptographic algorithm, as well as their comparison with the results obtained for the AES cryptographic algorithm, made it possible to establish that the developed cryptographic algorithm provides a sufficient level of information protection while requiring only two rounds. Therefore, the developed cryptographic algorithm for encrypting graphic information can be recommended for practical use, in particular, on resource-constrained platforms.

Keywords: cryptographic algorithm, image encryption, dynamic chaos, Hyper-Chaotic Modified Robust Logistic Map, Galois transform-based S-box, Nyberg construction.

Introduction and statement of the problem. Today, the development of information technologies adheres to increasing the amount of graphic information that is generated and transmitted. At the same time, the current state of computer technology involves the use of various devices for working with such information, including resource-constrained devices, such as mobile devices, IoT and IoBT devices, and embedded devices.

In modern information protection systems, cryptographic means are one of the most important tools that ensure confidentiality. At the same time, block symmetric ciphers, such as the AES cryptographic algorithm [1], are used to encrypt large volumes of information, including multimedia content. Nevertheless, today's cryptographic algorithms, which are adapted specifically for the encryption of multimedia information and allow for a significant reduction in the level of computing costs required for the encryption of multimedia, are actively developed and increasingly used in practice.

One of the most promising areas of development of such cryptographic algorithms is chaotic maps. Chaos is the pseudo-random and unpredictable motion exhibited by a deterministic dynamical system due to its sensitivity to input values and parameters. The research of chaos theory began with the three-body problem, which was researched by A. Poincare [3]. Today, many papers [4 – 7] are devoted to the research of the problems of

applying chaos theory to the encryption of multimedia information, however, the final optimal structure of cryptographic transformation based on chaotic maps has not been created yet.

The *purpose* of this paper is to improve the effectiveness of cryptographic protection of graphic information by developing a cryptographic algorithm based on chaotic map and Galois field transform.

Components of the proposed cryptographic algorithm. The proposed cryptographic algorithm uses a gamma block based on the theory of dynamic chaos, namely on the Hyper-Chaotic Modified Robust Logistic Map (HC-MRLM) [8]. For the completeness of the presentation of the material, we will briefly describe the algorithm of operation of this generator of pseudo-random key sequences.

Step 1. Set values $x_0 \in (0,1)$ and $\gamma \in [4,31]$.

Step 2. Calculate the values

$$\eta_1 = \left\lceil \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{\lfloor \gamma/4 \rfloor}{\gamma}} \right\rceil, \eta_2 = \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{\lfloor \gamma/4 \rfloor}{\gamma}} \right\rceil. \quad (1)$$

Step 3. Set the values of counters $i = 1$ and $j = 1$.

Step 4. If $\gamma \le 4$, calculate

$$x_i = \gamma x_{i-1}(1 - x_{i-1}), \quad (2)$$

otherwise, calculate

$$x_i = \begin{cases} \dfrac{\gamma x_{i-1}(1-x_{i-1})(\mathrm{mod}\,1)}{\gamma/4\,(\mathrm{mod}\,1)}, \text{ if } x_{i-1} \ge \eta_1 \; i \; x_{i-1} \le \eta_2 \\ \gamma x_{i-1}(1-x_{i-1})(\mathrm{mod}\,1), \text{ otherwise.} \end{cases} \quad (3)$$

Step 5. If $x_i \ge 0.1$ and $x_i \le 0.6$ calculate the temporary value

$$t = x_i \cdot 10^{10} (\mathrm{mod}\,1), \quad (4)$$

otherwise, increase the counter value $i = i + 1$ and go to *Step 4*.

Step 6. Based on the temporary value, calculate the gamma element

$$y_j = \begin{cases} 1, \text{ if } t \ge 0.5, \\ 0, \text{ if } t < 0.5. \end{cases} \quad (5)$$

Increase the value of the counter $j = j + 1$.

Step 7. If all necessary gamma elements are generated, exit the algorithm, otherwise, increase the value of the counter $i = i + 1$ and go to *Step 4*.

In the paper [8] the high cryptographic quality of such a generator is proved, as well as the high stochastic quality of the sequences generated by it. At the same time, the number of protection levels of the specified generator is greater than 2^{100}, which is sufficient for its use in information encryption tasks.

In addition to the generator of pseudorandom key sequences based on the chaotic map, the proposed cryptographic algorithm uses the S-box based on the Galois field transform [9] and the P-box, for which it is proposed to use a permutation which is based on the Nyberg construction over non-binary Galois fields [10].

Thus, as a nonlinear transformation of the cryptographic algorithm, it is proposed to use promising constructions of non-binary Galois fields, which were first described in [9] and are characterized by a high level of cryptographic quality. As part of the experiments performed in this paper, the S-box was used, which is the third row of the direct matrix of the Galois field transform, constructed using arithmetic, defined by the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x^2 + 1$

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	47	A7	D8	72	E0	3E	36	5F	92	4E	38	23	81	1A
1	83	A0	DE	90	AA	3D	9D	AD	0E	97	C1	13	67	16	88	30
2	E9	FB	28	D1	B9	C4	24	57	A4	C3	48	89	60	56	6C	ED
3	8D	52	EC	20	77	DB	CD	84	D0	70	8B	26	22	50	0C	AB
4	7D	85	F7	D2	0A	99	73	10	69	53	31	49	09	AC	DC	0B
5	29	71	F9	43	12	59	65	B8	18	DF	9B	BC	1B	54	7C	CC
6	64	C5	9A	95	3B	CE	08	9C	D4	42	FF	7F	74	FA	21	6D
7	34	C2	1C	82	EB	F2	87	E5	86	B1	14	3F	03	8F	E3	E7
8	58	C0	66	4C	F4	8E	BA	7A	8C	68	61	25	D5	F8	04	A6
9	5D	96	DD	98	4B	2A	55	80	45	93	2B	1E	37	41	CB	63
A	4D	17	5B	CA	79	DA	D9	11	8A	2C	51	39	5E	40	2E	6F
B	06	BB	FE	FC	EF	B3	2F	32	CF	A9	15	E1	1F	4A	33	6E
C	19	91	76	78	A8	3A	62	5A	C7	A2	BD	94	02	F5	27	2D
D	35	A5	9E	A3	F6	C8	D6	D7	1D	A1	B0	E4	4F	44	5C	0F
E	0D	3C	BE	B7	07	7B	AE	B6	F3	B4	B2	6A	E8	75	7E	FD
F	AF	BF	6B	EE	05	46	C6	9F	C9	D3	EA	B5	F1	E2	F0	E6

. (6)

S-box (6) is characterized by a high level of nonlinearity, a small deviation from compliance with the strict avalanche criterion, uniform minimization of the elements of the correlation coefficients matrix, which makes it a promising choice for use in the proposed cryptographic algorithm.

Note that the inverse substitution to substitution (6) has the following form

S^{-1}	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	CC	7C	8E	F4	B0	E4	66	4C	44	4F	3E	E0	18	DF
1	47	A7	54	1B	7A	BA	1D	A1	58	C0	0F	5C	72	D8	9B	BC
2	33	6E	3C	0D	26	8B	3B	CE	22	50	95	9A	A9	CF	AE	B6
3	1F	4A	B7	BE	70	D0	08	9C	0C	AB	C5	64	E1	15	07	7B
4	AD	9D	69	53	DD	98	F5	02	2A	4B	BD	94	83	A0	0B	DC
5	3D	AA	31	49	5D	96	2D	27	80	55	C7	A2	DE	90	AC	09
6	2C	8A	C6	9F	60	56	82	1C	89	48	EB	F2	2E	6F	BF	AF
7	39	51	05	46	6C	ED	C2	34	C3	A4	87	E5	5E	40	EE	6B
8	97	0E	73	10	37	41	78	76	1E	2B	A8	3A	88	30	85	7D
9	13	C1	0A	99	CB	63	91	19	93	45	62	5A	67	16	D2	F7
A	11	D9	C9	D3	28	D1	8F	03	C4	B9	14	3F	4D	17	E6	F0
B	DA	79	EA	B5	E9	FB	E7	E3	57	24	86	B1	5B	CA	E2	F1
C	81	1A	71	29	25	61	F6	C8	D5	F8	A3	9E	5F	36	65	B8
D	38	23	43	F9	68	8C	D6	D7	04	A6	A5	35	4E	92	12	59
E	06	BB	FD	7E	DB	77	FF	7F	EC	20	FA	74	32	2F	F3	B4
F	FE	FC	75	E8	84	CD	D4	42	8D	52	6D	21	B3	EF	B2	6A

. (7)

As a P-box, it is proposed to use a permutation built on the basis of Nyberg construction [10], in which each element is defined as the multiplicative inversion of the given element by a double modulus

$$y_i = x_i^{-1} \bmod(3, \psi(x)),\ x_i \in GF(3^5),\ i = 0,1,...,242, \quad (8)$$

where the irreducible over $GF(3)$ polynomial $\psi(x) = x^5 + 2x + 1$ is chosen.

The permutation itself has the following form

$$P = \{0,1,2,163,210,240,83,120,150,217,57,60,70,104,200,80,115,142,110,30,33,\\ 40,194,221,50,154,178,235,98,37,19,58,216,20,218,62,183,29,117,114,21,143,\\ 149,140,136,106,88,172,198,103,24,207,229,202,119,74,184,10,31,109,11,108,\\ 35,176,101,167,144,161,134,153,12,179,96,234,55,214,191,196,219,193,15,241,\\ 212,6,112,188,180,175,46,99,169,186,111,182,170,113,72,118,28,89,105,64,155,\\ 49,13,100,45,165,61,59,18,92,84,95,39,16,192,38,97,54,7,211,162,127,204,233,\\ 129,123,157,126,238,205,208,201,68,195,44,215,189,213,43,220,17,41,66,203,\\ 228,197,190,42,8,164,242,69,25,102,239,128,232,230,209,67,122,3,151,107,\\ 171,65,224,90,94,166,47,174,173,87,63,199,26,71,86,222,93,36,56,236,91,223,\\ 85,138,148,76,116,79,22,135,77,147,48,177,14,133,53,145,124,131,226,51,132,\\ 160,4,121,82,139,75,137,32,9,34,78,141,23,181,187,168,231,206,237,146,52,\\ 159,225,158,125,73,27,185,227,130,156,5,81,152\}, \tag{9}$$

while the inverse permutation for permutation (9) has the following form

$$P^{-1} = \{0,1,2,163,210,240,83,120,150,217,57,60,70,104,200,80,115,142,110,30,\\ 33,40,194,221,50,154,178,235,98,37,19,58,216,20,218,62,183,29,117,114,\\ 21,143,149,140,136,106,88,172,198,103,24,207,229,202,119,74,184,10,31,109,\\ 11,108,35,176,101,167,144,161,134,153,12,179,96,234,55,214,191,196,219,193,\\ 15,241,212,6,112,188,180,175,46,99,169,186,111,182,170,113,72,118,28,89,105,\\ 64,155,49,13,100,45,165,61,\ 59,18,92,84,95,39,16,192,38,97,54,7,211,162,127,\\ 204,233,129,123,157,126,238,205,208,201,68,195,44,215,189,213,43,220,17,41,\\ 66,203,228,197,190,42,8,164,242,69,25,102,239,128,232,230,209,67,122,3,151,\\ 107,171,65,224,90,94,166,47,174,173,87,63,199,26,71,86,222,93,36,56,236,91,\\ 223,85,138,148,76,116,79,22,135,77,147,48,177,14,133,53,145,124,131,226,51,\\ 132,160,4,121,82,139,75,137,32,9,34,78,141,23,181,187,168,231,206,237,146,\\ 52,159,225,158,125,73,27,185,227,130,156,5,81,152\}. \tag{10}$$

The algorithms for information encryption and decryption. On the basis of mentioned cryptographic primitives, an effective algorithm for encrypting digital images consisting of two rounds was proposed.

In addition to the application of chaotic map, effective S-boxes based on Galois field transform and P-boxes based on permutations generated using the Nyberg construction, in the proposed information encryption algorithm an approach that involves working with three-dimensional image blocks is used, which allows a higher level of diffusion.

Information encryption algorithm:

Input data: a three-dimensional matrix of the input image P of size $m \times n \times 3$, the elements of which are integer numbers in the range $[0,255]$, initial data x_0 and γ for the chaotic map, a specific type of substitution S, a specific type of permutation P.

Output data: a three-dimensional encrypted image matrix C of size $m \times n \times 3$, the elements of which are integer numbers in the range $[0,255]$.

Encryption algorithm:

Step 1. Segment the image into three-dimensional blocks of size $9 \times 9 \times 3$. If the size of the image is not a multiple of the size of the block, the side blocks are supplemented with elements from the blocks lying on the opposite side of the image.

Step 2. The iteration counter of the rounds is set as $\alpha = 0$.

Step 3. Substitution within the block. Sequentially, in each block, the elements of the blocks are replaced according to the rule defined by substitution S.

Step 4. Permutation within the block. Each block of size $9 \times 9 \times 3$ is represented as a one-dimensional sequence $\{u_i\}, i = 0,1,...,242$ by sequential concatenation of columns taken sequentially from each matrix in the third dimension. Next, the permutation of elements is applied to the resulting sequence $\{u_i\}$ according to the rule defined by permutation P. After permuting the elements of the sequence $\{u_i\}$, the formation of an

encrypted block is performed by successively filling it by columns, and then by filling each of the matrices of the third dimension with the elements of the sequence $\{u_i\}$.

Step 5. Gamming within the image. The image matrix is represented as a sequence $\{g_i\}, i = 0,1,...,m \cdot n \cdot 3 - 1$ by successive concatenation of columns that are taken sequentially from each matrix in the third dimension. The gamming result is determined in the following way

$$r_i = \begin{cases} g_i \oplus y_i, \text{ if } i = 0, \\ g_i \oplus g_{i-1} \oplus y_i, \text{ if } i \neq 0. \end{cases} \quad (11)$$

where y_i is the next bit of the gamma generated by the generator based on the Hyper-Chaotic Modified Robust Logistic Map, the notation $\oplus$ means the bitwise sum modulo 2, and $i = 0,1,...,m \cdot n \cdot 3 - 1$. After gamming, the resulting matrix of the image is formed from the sequence $\{r_i\}$ by sequentially filling it by columns, and then by filling each of the matrices of the third dimension, with elements of the sequence $\{r_i\}$.

Step 6. Increase the counter of the rounds $\alpha = \alpha + 1$. If $\alpha = 2$ the image encryption is complete, otherwise go to *Step 3*.

Information decryption algorithm:

Input data: a three-dimensional matrix of an encrypted image C of size $m \times n \times 3$, whose elements are integer numbers in the range $[0,255]$, initial data x_0 and γ for the chaotic map, a specific type of inverse substitution S^{-1}, a specific type of inverse permutation P^{-1}.

Output: a three-dimensional matrix of the output image P of size $m \times n \times 3$, whose elements are integer numbers in the range $[0,255]$.

Decryption algorithm:

Step 1. Segment the image into three-dimensional blocks of size $9 \times 9 \times 3$. If the size of the image is not a multiple of the size of the blocks, the blocks are supplemented with elements from the blocks lying on the opposite side of the image.

Step 2. The iteration counter of the rounds is set $\alpha = 0$.

Step 3. Gamming within the image. The image matrix is represented as a sequence $\{g_i\}, i = 0,1,...,m \cdot n \cdot 3 - 1$ by successive concatenation of columns that are taken sequentially from each matrix in the third dimension. After gamming, the resulting matrix of the image is formed from the sequence $\{r_i\}$ by sequentially filling it by columns, and then by filling each of the matrices of the third dimension, with elements of the sequence $\{r_i\}$.

Step 4. Reverse permutation within the block. Each block of size $9 \times 9 \times 3$ is represented as a one-dimensional sequence $\{u_i\}, i = 0,1,...,242$ by sequential concatenation of columns taken sequentially from each matrix in the third dimension. Next, permutation of elements is applied to the resulting sequence $\{u_i\}$ according to the rule defined by permutation P^{-1}. After permuting the elements of the sequence $\{u_i\}$, the decrypted block is formed by successively filling it by columns, and then by filling each of the matrices of the third dimension with elements of the sequence $\{u_i\}$.

Step 5. Reverse substitution within the block. Sequentially, in each block, the elements of the block are replaced according to the rule defined by inverse substitution S^{-1}.

Step 6. Increase the counter of the rounds $\alpha = \alpha + 1$. If $\alpha = 2$ the image decryption is complete, otherwise go to *Step 3*.

We show in Fig. 1 a schematic representation of the proposed cryptographic algorithm for encryption and decryption of digital images.

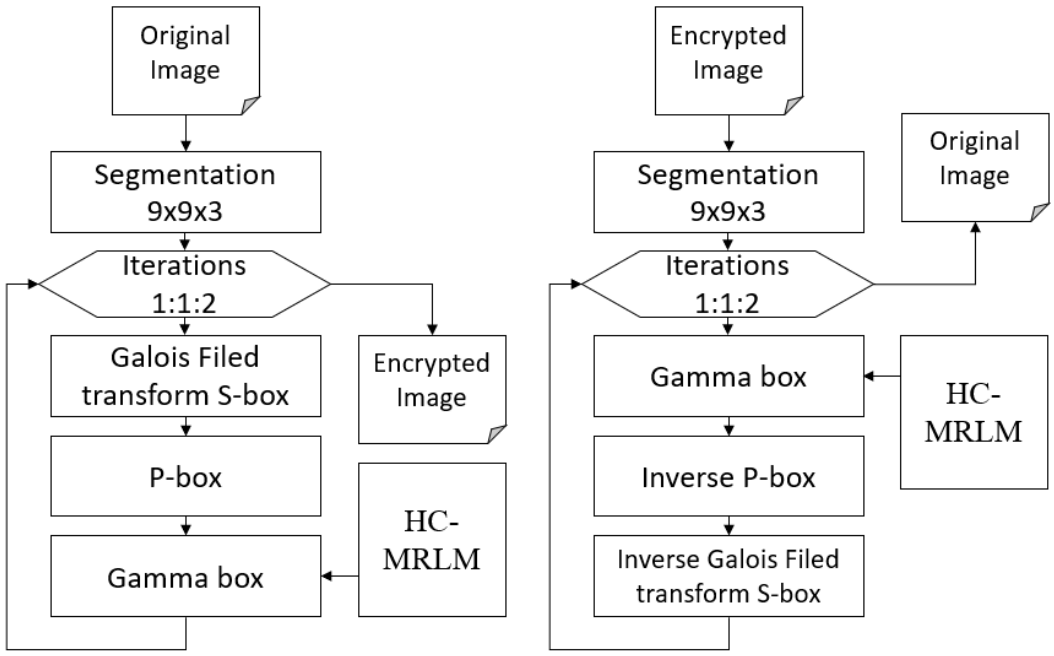


Fig. 1. Schematic presentation of the proposed cryptographic algorithm

Testing results of the proposed cryptographic algorithm. The proposed cryptographic algorithm for image encryption due to its optimal structure, which is adapted for the encryption of graphic information, as well as the high quality of the cryptographic primitives included into its composition, allows us to achieve sufficient results in the encryption of graphic information. In Fig. 2 we present an example of the original and encrypted digital image using the proposed cryptographic algorithm.

Fig. 2. An example of the original and encrypted image

For a deeper assessment of the quality of cryptograms obtained using the developed cryptographic algorithm, a NIST stochastic tests suite [11] can be used, which consists of 15 tests designed to determine the stochastic properties of binary sequences. A high-quality encryption algorithm should produce output sequences that are indistinguishable from truly random sequences.

To test the quality of the developed cryptographic algorithm, the following experiment was performed: 250 images from the NRCS database [12] were encrypted with the AES cryptographic algorithm (2 rounds), the AES cryptographic algorithm (14 rounds), and the proposed cryptographic algorithm. After encryption, the resulting cryptograms were truncated to a size of 1 MB and tested with the NIST stochastic test

suite. A set of tests was considered passed if all tests from the set were passed. The results of the experiment are presented in the Table 1. In the Table 1, the information shown is interpreted as the number of cryptograms that did not pass the NIST test suite / the total number of cryptograms.

Table 1

Results of experimental testing of the developed graphic information encryption algorithm

The proposed cryptographic algorithm(2 rounds) *Failed / Total number*	AES(2 rounds) *Failed / Total number*	AES(14 rounds) *Failed / Total number*
56/250	61/250	47/250

Analysis of the data presented in the Table 1 allows us to conclude about the significant effectiveness of the proposed cryptographic algorithm for encrypting graphic information, which is sufficient for most practical applications. Although more cryptograms pass the NIST test suite when applying AES with 14 rounds, it should be noted that 14 rounds involve a large amount of computation, while the proposed cryptographic algorithm involves only 2 rounds of the SP network.

Conclusions. Let's note the main results of the research performed:

1. Common use of graphic information in modern cyberspace, combined with the widespread use of resource-constrained devices, in particular IoT devices, IoBT devices, mobile platforms, leads to the high importance of the issue of developing high-speed cryptographic algorithms for encrypting graphic information.

2. In this paper we propose an algorithm for encrypting graphic information based on a Hyper-Chaotic Modified Robust Logistic Map, as well as an SP network, which includes an S-box based on a Galois field transform, as well as a P-box based on a permutation, synthesized using the Nyberg construction.

3. Testing of cryptograms obtained using the developed cryptographic algorithm using a NIST stochastic tests suite shows that it allows to ensure a sufficient level of information protection while requiring only two rounds.

References

1. FIPS 197. Advanced encryption standard. 2001. URL: http://csrc.nist.gov/publications/
2. Kumari M., Gupta S., Sardana P. A survey of image encryption algorithms. *3D Research*. 2017. Vol. 8. P. 1-35.
3. Poincare H. J. Les methodes nouvelles de la mecanique celeste (Gauthiers-Villars, Paris, 1892, 1893, 1899). V. 1–3. [English translation edited by D. Goroff. New York: American Institute of Physics, 1993].
4. Zhang Y. The fast image encryption algorithm based on lifting scheme and chaos. *Information sciences*. 2020. V. 520. P. 177-194.
5. Pourasad Y., Ranjbarzadeh R., Mardani A. A new algorithm for digital image encryption based on chaos theory. *Entropy*. 2021. V. 23, No. 3. 341.
6. Luo Y. et al. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*. 2019. V. 78. P. 22023-22043.
7. He Y. et al. A new image encryption algorithm based on the OF-LSTMS and chaotic sequences. *Scientific reports*. 2021. V. 11, 6398.
8. Irfan M. et al. Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM*). Electronics*. 2020. V. 9. No. 1. 104.
9. Bakunina O.V., Balandina N.M., Sokolov A.V. Synthesis Method for S-boxes Based on Galois Field Transform Matrices. *Ukrainian Journal of Information Technology*. 2023. V.5, No 2. P. 41–48.

10. Zhdanov O.N., Sokolov A.V. Extending Nyberg construction on Galois fields of odd characteristic. *Radioelectronics and Communications Systems*. 2017. V. 60, No. 12. P. 538-544.
11. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000. 153 p.
12. NRCS Photo Gallery. United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

АЛГОРИТМ ШИФРУВАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ХАОТИЧНОГО ПЕРЕТВОРЕННЯ І GF-ПЕРЕТВОРЕННЯ

О.О. Палагін, А.В. Соколов

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: radiosquid@gmail.com

Сучасний етап розвитку інформаційних технологій характеризується суттєвим збільшенням обсягів мультимедійної інформації, зокрема, цифрових зображень при повсюдному впровадженні ресурсообмежених платформ, таких, як пристрої IoT, IoBT, мобільні пристрої та вбудовані системи. Зазначене обумовлює актуальність завдання розробки алгоритмів шифрування графічної інформації, які були б здатні забезпечити високу ефективність шифрування інформації за найменшу кількість обчислювальних операцій. На сьогодні для розробки таких криптографічних алгоритмів найчастіше застосовується теорія динамічного хаосу. Тим не менш остаточно оптимальної структури криптографічного алгоритму для шифрування зображень на сьогодні ще не створено. У даній роботі запропоновано комбінацію переваг традиційних SP мереж та генератора гами на основі гіперхаотичної модифікованої стійкої логістичної карти для побудови ефективного алгоритму шифрування зображень, що здатний забезпечити високий рівень стійкості. У запропонованому криптографічному алгоритмі застосовуються високоякісні S-блоки на основі GF-перетворення, а також P-блоки на основі перестановок, що згенеровані із застосуванням конструкції Ніберг, при цьому застосовується сегментація і подальша обробка тривимірних блоків зображень, що дозволяє збільшити ефект дифузії. Проведені в рамках роботи численні тести стохастичної якості криптограм, отриманих із застосуванням розробленого криптографічного алгоритму, а також їх порівняння із результатами, отриманими для криптографічного алгоритму AES дозволили встановити, що розроблений криптографічний алгоритм дозволяє забезпечити достатній рівень захисту інформації, при цьому вимагає всього два раунди основного кроку криптоперетворення. Отже, розроблений криптографічний алгоритм для шифрування графічної інформації може бути рекомендований для практичного застосування, зокрема, на ресурсообмежених платформах.

Ключові слова: криптографічний алгоритм, шифрування зображень, динамічний хаос, гіперхаотична модифікована стійка логістична карта, S-блок на основі GF-перетворення, конструкція Ніберг.

DOI 10.15276/imms.v13.no3-4.212
UDC 681.51

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 212-218

NON-CLASSICAL METHOD OF CALCULATING THE INTEGRAL COMPONENT IN REGULATORS OF MULTIVARIABLE DISCRETE-TIME CONTROL SYSTEMS

O.A. Stopakevych[1], A.O. Stopakevych[2]

[1] National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
[2] State University of Intellectual Technologies and Telecommunications
1, Kuznechna, 65000, Odesa, Ukraine
e-mail: stopakevich@gmail.com

A new method of designing controllers with an integral term as part of multivariable optimal control systems in discrete time is proposed. Traditional methods of designing multivariable controllers have been investigated, and a prototype of the controller has been chosen as a basis for comparison. Specific formulas for design of the proposed controller are given. Comparing the transition processes of the control systems outputs with a unit-step disturbance at the plant input using the proposed controller and optimal controller obtained by the typical method, it can be concluded that the proposed controller compensates the disturbance and gives a faster transition process. The main feature of the proposed method is that, for multivariable systems with a large number of inputs and outputs, it significantly simplifies the design of the controller. This is because it does not require the extension of the plant state matrix by the number of inputs at the transfer of the matrices to the optimal controller design programs.
Keywords. MIMO optimal controller, integral term, new design method, computational simplification of design.

Analysis of the problem. It is known that the integral component in regulators performs an important function in ensuring the accuracy of reference maintenance and compensation of disturbances in control systems. Let us briefly consider the implementation options of the integral component in multidimensional optimal control systems in discrete time.

Let's define a multidimensional control plant in the state space in the form

$$x_{i+1} = A \cdot x_i + B \cdot u_i + B \cdot f_i$$

$$y_i = C \cdot x_i$$

We'll assume that the plant under consideration has the same number of inputs and outputs.

Let's consider the main options for including integrators in the controllers of multivariable discrete control systems [1-5] (Fig. 1).

The simplest is option **1**. Here, a multivariable discrete integrator is simply included in parallel with the state controller. Accordingly, it is optimal according to the integral criterion

$$J = \frac{1}{2}\sum_{i=0}^{\infty} x_i^T \cdot Q \cdot x_i + u_i^T \cdot R \cdot u_i$$

MIMO state controller can be designed with the MATLAB function C1=dlqr(Ad,Bd,Q,R). Accordingly, the optimal multivariable state controller is calculated using the MATLAB program Ad1=[Ad zeros(n,m); C eye(m)]; Bd1=[Bd; zeros(m)]; [Kd,P]=dlqr(Ad1,Bd1,Q,R); C1=Kd(m:n);C2=Kd(m, n+m);

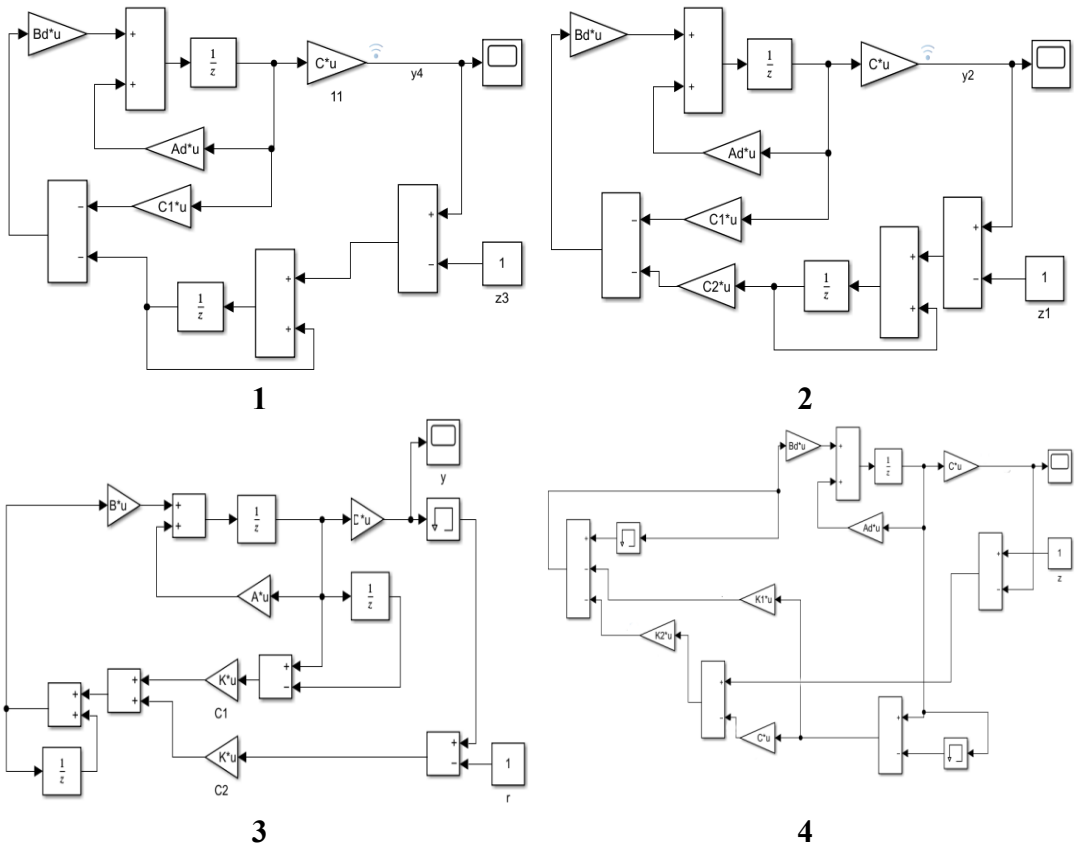


Fig 1. Diagrams of the main options of integral action realization in discrete MIMO control systems

The main options for including integrators in the controllers of multivariable discrete systems.

In option **2**, the parameters of the I-component are determined by the extended matrix

$$\begin{bmatrix} x_{i+1} \\ q_{i+1} \end{bmatrix} = \begin{bmatrix} A & 0 \\ C & I \end{bmatrix} \cdot \begin{bmatrix} x_i \\ q_i \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} \cdot u_i + \begin{bmatrix} B \\ 0 \end{bmatrix} \cdot f_i$$

In option **3**, the control is implemented in the velocity or differential form. The control law has the form (r is the reference)

$$u_i = u_{i-1} + C_1 \cdot x_i + C_2 \cdot (y_{i-1} - r).$$

This implementation is less accepted, but it has one advantage, namely there is the ability to limit the rate of change of state variables and control actions.

Option **4** is quite effective, but structurally more complex.

Let's introduce optimality criterion in the form:

$$J = \frac{1}{2} \sum_{i=0}^{\infty} e_i^T \cdot Q \cdot e_i + \Delta u_i^T \cdot R \cdot \Delta u_i,$$

where $\Delta u_i = u_i - u_{i-1}, e_i = r - y_i$

Determining , $\Delta x_{i+1} = x_{i+1} - x_i$, the system can be written in the form

$$\Delta x_{i+1} = A \cdot \Delta x_i + B \cdot \Delta u_i$$
$$\Delta y_i = C \cdot \Delta x_i$$

By entering the vector $e_{i+1} = e_i - C \cdot \Delta x_{i+1}$, we will get the standard problem of controller design

$$K = (K_1, K_2) = dlqr(A1, B1, Q1, R),$$

$$A1 = \begin{pmatrix} A & 0 \\ -C \cdot A & I \end{pmatrix}, \quad B1 = \begin{pmatrix} B \\ -C \cdot B \end{pmatrix}, \; Q1 = \begin{pmatrix} 0 & 0 \\ 0 & Q \end{pmatrix}$$

Thus, the controller can be written as $\Delta u_i = -K \cdot \Delta x_i$. Decomposing the matrix *K* into blocks *K=[K1 K2],* the controller can be rewritten in the form $u_i = u_{i-1} - K_1 \cdot \Delta x_i - K_2 \cdot e_i$ or, which is also the same,

$$u_i = -K_1 \cdot x_i - K_2 \cdot \sum_{j=0}^{i} e_j$$

The program code for the controller matrix calculation has the following form:

```
A1=[A zeros(n,m); -C*A eye(m)];
B1=[B;-C*B];
Q1=[zeros(m,n+m); zeros(n,m) Q];
K=dlqr(A1,B1,Q1,R);
K1=K(m:n);   K2=K(m,n+1:m+n);
```

Thus, the control law for the system can be written as $\Delta u_i = -K \cdot \Delta x_i$. Decomposing the matrix *K* into blocks *K=[K1 K2]*, the controller can be rewritten in the form or, which is also the same, $u_i = u_{i-1} - K_1 \cdot \Delta x_i - K_2 \cdot e_i$

In option **4,** the control problem is reduced to finding four unknown matrices $K,\ L,\ M,\ N$

$$L \cdot B \cdot R \cdot B^T \cdot M - Q = 0;$$

$$(L \cdot B \cdot R \cdot B^T \cdot N) + K + L \cdot A = 0;$$

$$-(N \cdot B \cdot R \cdot B^T \cdot M) + K + A^T \cdot M = 0;$$

$$-(N \cdot B \cdot R \cdot B^T \cdot N) + M + N \cdot A + L + A^T \cdot N = 0$$

To solve the system it is necessary to use optimization algorithms. For example, the YALMIP library allows to conveniently solve optimization problems and is focused on control system design. This library works in both MATLAB and Octave. The software implementation of the optimization problem has the following form.

```
A=[-0.313 56.7 0;-0.0139 -0.426 0;0 56.7 0];
B=[0.232;0.0203;0];C=[0 0 1]; D=0;
Q=1diag([1 1 5e2]); R=1/10; % inv(R)
L=sdpvar(3,3,'full'); K=sdpvar(3,3,'full');
M=sdpvar(3,3,'full'); N=sdpvar(3,3,'full');
eps=0.01;
Constraints = [0<=y1<=eps;0<=y2<=eps,0<=y3<=eps;0<=y4<=eps;];
sol = optimize(Constraints);
N1=double(N);M1=double(M);
KP=inv(R)B'N1; KI=inv(R)B'*M1;
```

It should be noted that the solution of even a relatively simple problem is not trivial. The problem is not solved for all possible *R* and *Q*. There is a fairly high chance of obtaining an unstable system due to the presence of an imprecise solution. Since, as a rule, in order to achieve a significantly different result, the weight matrices coefficients should be significantlly changed, the greater the difference between the coefficients, the less accurate the solution. Therefore, it is quite difficult to apply the

given option as a universal one. Nevertheless, this option has one advantage: the integral component is found based on the criterion of optimality.

To compare the action of the considered options, we will simulate them. To do this, let's set the object model in the form with one input and one output (to simplify the analysis of responces) in the form Ac=[-0.313 56.7 0; -0.0139 -0.426 0; 0 56.7 0]; Bc=[0.232;0.0203;0]; C=[0 0 1]; D=0; dt=1; [A B]=c2d(Ac,Bc,dt); Q=diag([1 1 1]); R=1. Graphs of responces are shown in Fig. 2.

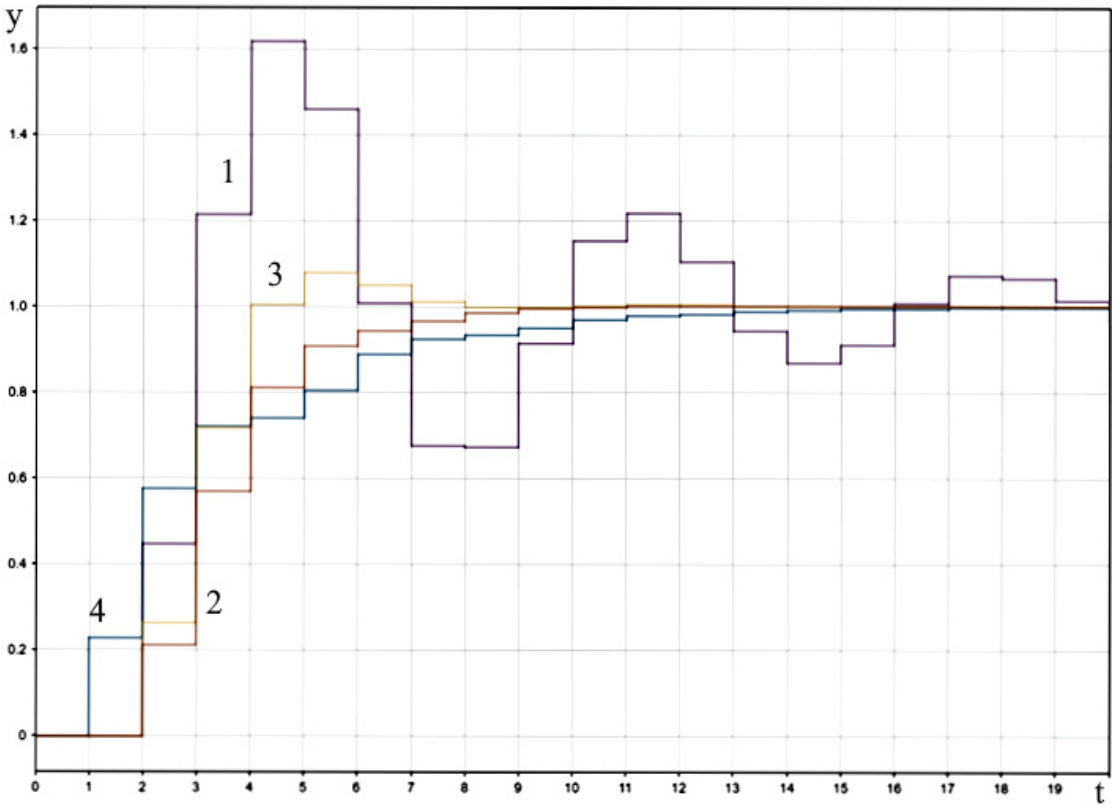


Fig. 2. Comparison of the closed-loop control systems simulation results using controllers of
options 1 –4

The figure shows that the use of a simple integrator (option 1) significantly reduces the control quality. Other options in the given example give approximately the same results. Therefore, for further research, we will choose the typical (simpler) option 2.

Main part. Instead of the typical state space expansion procedure used in the description of option 2, we offer a modified procedure: synthesize a standard optimal state controller *K*, and then find the matrix of the integral component *KK* according to the formula

$$KK = \left(K \cdot A - W \cdot B^T \quad W + K \cdot B - I\right) \cdot \begin{pmatrix} A - I & B \\ C & 0 \end{pmatrix}^{-1},$$

where *W* is a positive definite diagonal tuning matrix. The controller is given by the formula

$$u_{i+1} = u_i - K1 \cdot (x_{i-1} - x_i) - K2 \cdot y_i$$
$$K1 = KK(m, 1:n), K2 = KK(m, n+1:n+m)$$

To study the transition processes with the proposed controller, we will choose a simple plant in discrete time, which in the state space is defined by matrices with the sample time dt=1.

$$A=\begin{pmatrix}0.5 & 0.2\\ 0.1 & 0.4\end{pmatrix}, B=\begin{pmatrix}1\\ 2\end{pmatrix}, C=\begin{pmatrix}3 & 4\end{pmatrix}$$

In the form of a transfer function, the plant has the form

$$W(z)=\frac{11\cdot z-3.6}{z^2-0.9\cdot z+0.18}$$

The plant step response is shown in Fig. 3

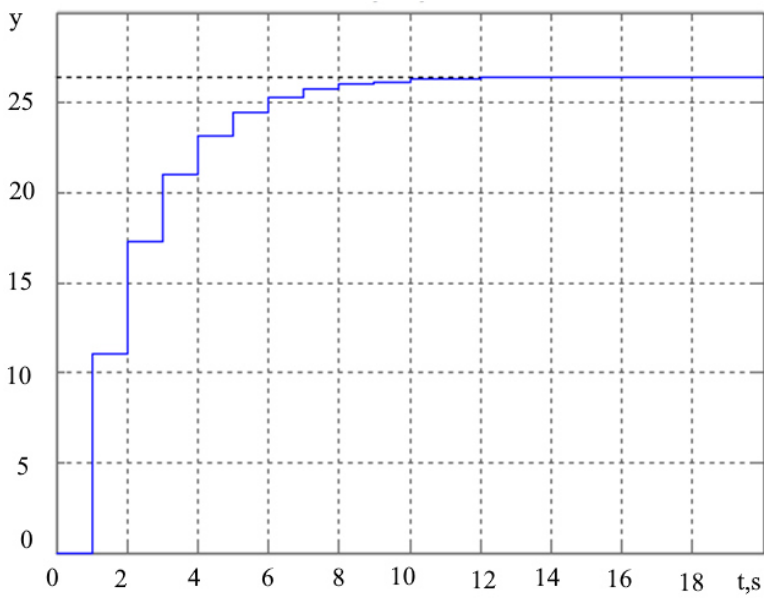


Fig. 3. The plant step response

Let's design the proposed controller by choosing

Q=1000*eye(2), R=1, W=0.14;

K=dlqr(A,B,Q,R);

KK=[K*A-W*B' W+K*B-1]*inv([A-eye(2) B; C 0]);

As a result, we get

KK=(-0.1816 -0.0628 -0.0427), K1=(-0.1816 -0.0628), K2=-0.0427.

The transient processes of output and control in a closed-loop control system with the proposed controller are shown in Fig. 4.

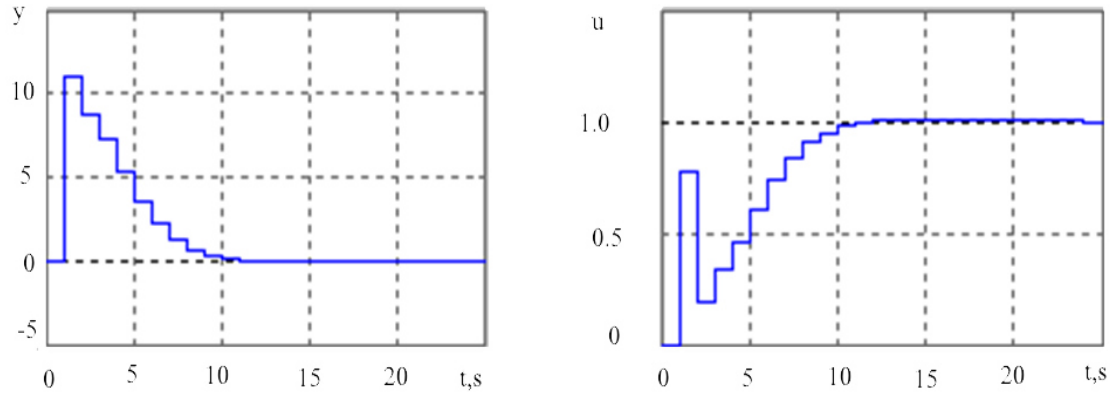


Fig. 4. Transient processes of output and control under a step disturbance in a closed-loop control system with the proposed controller

For comparison, Fig. 5 shows transient processes with the initial optimal static controller *K*.

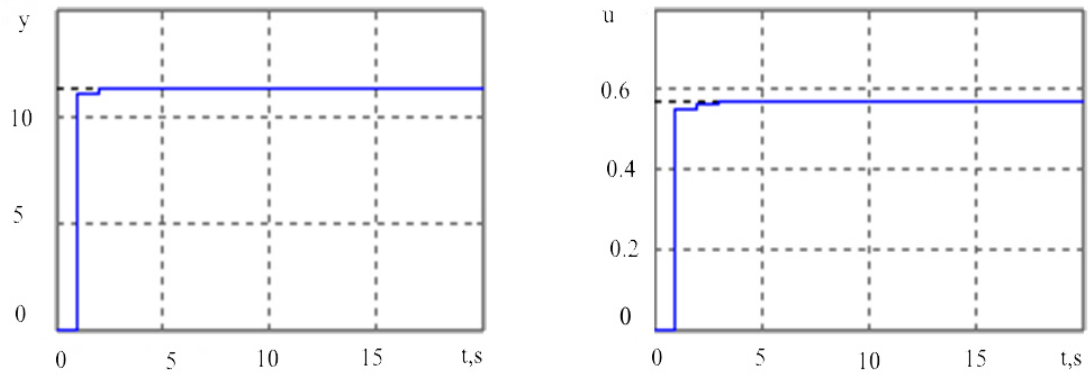


Fig. 5. The output transient processes in the closed-loop control system with the optimal static controller

Conclusions. To draw conclusions, we will compare the obtained responses with the responses in the system that uses a typical controller of option 2. For this, we will use the program code

AI=[A zeros(2,1);C 1]; BI=[B;0];
QI=[1000 0 0; 0 1000 0; 0 0 1]; RI=1;
KI=dlqr(AI,BI,QI,RI);
KI1=KI(1:2); KI2=KI(3);

We get KI= – (0.1954 0.2513 0.0128), KI1=-(0.1954 0.2513); KI2=–0.0128.

From the comparison of the responses in the control system at the output when using the proposed (1) and typical (2) controllers, it can be concluded that the proposed controller qualitatively compensates for the disturbance and provides a faster response. At the same time, for MIMO systems with a large number of inputs and outputs, it significantly simplifies the controller design, as it does not require the expansion of the matrix of plant states by the number of inputs before transferring the matrices to the design program (for example, dlqr).

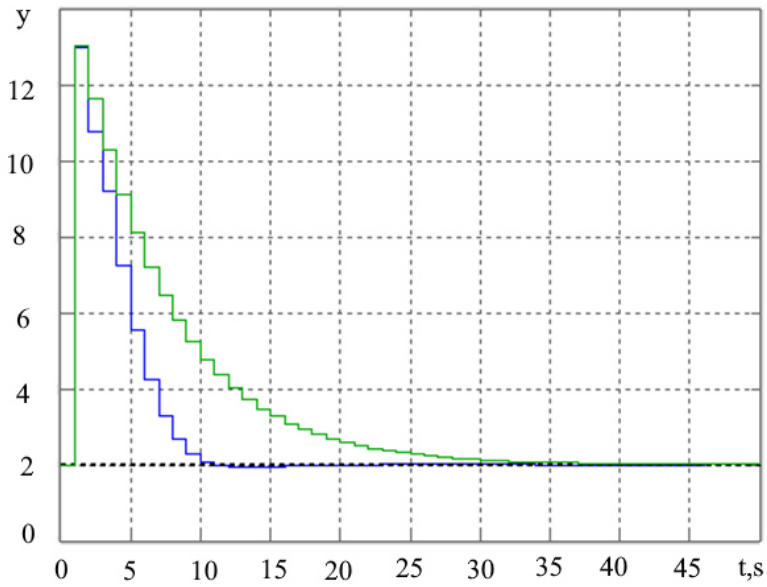


Fig. 6. Comparison of the closed-loop control systems simulation results using the proposed (1) and typical (2) controllers

References

1. Stopakevych A.A. System analysis and theory of complex control systems. Odesa: Astroprint, 2013 (in Russian)
2. Isermann R. Digital Control Systems. New York: Springer-Verlag, 1981.

3. Tan W., Han W., Xu J. State-Space PID: A Missing Link Between Classical and Modern Control. *IEEE Access*. 2022. V.10. P.116540 – 116553. DOI 10.1109/ACCESS.2022.3218657
4. Stopakevych A.O. Solving the saturation problem in control systems with PID-type controllers with an integral component included. *Economics and management in the conditions of building an information society. X International Conference*. Odesa: SUITT, 2021. P.89-93. (in Ukrainian)
5. Ruscio D. Discrete LQ optimal control with integral action: A simple controller on incremental form for MIMO systems. *Modeling, Identification and Control*. 2012. V. 33. No. 2. P. 35–44.

НЕКЛАСИЧНИЙ МЕТОД РОЗРАХУНКУ ІНТЕГРАЛЬНОЇ СКЛАДОВОЇ В РЕГУЛЯТОРАХ БАГАТОВИМІРНИХ СИСТЕМ УПРАВЛІННЯ В ДИСКРЕТНОМУ ЧАСІ

О.А. Стопакевич[1], А.О. Стопакевич[2]

[1] Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
[2] Державний університет інтелектуальних технологій і зв'язку
1, Кузнечна, Одеса, 65000, Україна
e-mail: stopakevich@gmail.com

Запропоновано новий метод розрахунку регуляторів з інтегральною складовою в складі багатовимірних оптимальних систем управління в дискретному часі. Проаналізовано традиційні методи розрахунку багатовиірних регуляторів, та обрано варіант регулятора як базу для порівняння. Приведені конкретні формули розрахунку запропонованого регулятора. З порівняння процесів в системі управління по виходу при одиничному збуренні по входу об'єкта при використанні запропонованого та синтезованого за типовим методом оптимальних регуляторів можна зробити висновок, що запропонований регулятор якісно компенсує збурення і дає більш швидкий процес. Основною особливістю запропонованого метода є то, що для багатовимірних систем з великою кількістю входів і виходів він суттєво спрощує обчислення регулятора, оскільки не потребує розширення матриці станів об'єкта на число входів при передачі матриць в програми синтезу оптимальних регуляторів.
Ключові слова. MIMO оптимальний регулятор, інтегральна складова, новий метод розрахунку, обчислювальне спрощення синтезу.

DOI 10.15276/imms.v13.no3-4.219
UDC 004.9

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No.3-4, pp. 219-227

INTELLIGENT SYSTEM FOR SUPPORTING DECISION MAKING FOR ASSESSING THE TECHNICAL CONDITION OF COMPLEX SYSTEMS

A.V. Vychuzhanin

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
e-mail: v.v.vychuzhanin@op.edu.ua

The relevance of the topic is due to the need to make decisions to ensure the reliability of elements and assemblies of complex technical systems with insufficient information about their technical condition. The problem being solved is semi-structured and interdisciplinary. The effectiveness of solving the problem lies in the use of information technologies and artificial intelligence methods, in particular expert systems. The advantages of using information technologies to automate the decision-making process to assess the current technical condition of complex systems are considered. An intelligent decision support system has been developed that allows assessing the risk of failure of elements and components of complex technical systems using elements of artificial intelligence. The proposed decision support system contains: a database; a knowledge base with methods for calculating reliability indicators (probabilities and risks of failures) and a set of decision rules for selecting appropriate decision-making methods; results of determining the probabilities and risks of failure of elements and assemblies of complex technical systems with their ranking; intellectualization model for assessing the technical condition of elements and assemblies. The proposed algorithm for the functioning of a decision support system implements the task of automating the process of assessing the technical condition of complex systems. The use of the proposed decision support system for assessing the technical condition of complex systems will improve the reliability of technical systems with insufficient information about their technical condition.

Keywords: information technology, algorithm, complex technical systems, decision support, intelligent systems, artificial intelligence, expert systems, knowledge base, database, algorithm, complex technical systems, reliability, risk of failure, ship's power plant

Introduction. One of the significant problems of ensuring the reliability of complex technical systems (CTS) with insufficient information about their technical condition (TC) is the search for ways to increase the reliability and accuracy of assessing the reliability indicators of elements and components of technical systems. During the operation of CTS systems go through the following stages of TC changes: defect; damage; destruction; refusal.

Due to the increasing complexity of technical systems and the growing requirements for their reliability, the importance of the problem of access to the volumes of diagnostic information on reliability accumulated at various stages of CTS operation is increasing [1.2,3,4].

Currently, significant information materials have been accumulated containing methods for reliability research, as well as methods and models for assessing the reliability of CTS of various types.

A feature of the field of knowledge devoted to the problem of reliability is that most of the knowledge is the personal experience of experts in the field of reliability of CTS [4]. However, experts are often forced to make management decisions to ensure the reliability of CTS in the face of insufficient information about the technical condition of such systems. When assessing reliability, it is also necessary to take into account the

fact that CTS are characterized by a large number of diagnosed parameters that differ in information content and degree of accessibility. Such CTS are characterized by specific and varied operating conditions.

It is also significant that research and assessment of reliability indicators of such systems is characterized by decision-making under significant uncertainty, and often still requires significant material and time costs [5].

The growing complexity of technical systems, the variety of their parameters and insufficient information description of the state of the systems require improvement of management decisions to ensure the reliability of elements and components of systems based on the results of assessing their technical condition.

Thus, during the operation of CTS, the urgent task remains to improve methods aimed not only at assessing the technical condition of systems and the decisions made related to them, but at supporting the decisions made.

Objective and objectives of the study. To assess the reliability of CTS, various methods have been developed and used, often based on the methods of probability theory and mathematical statistics, which makes it possible to automate the process of assessing the reliability of elements and components of complex systems. However, the stages associated with supporting decisions made to ensure reliability based on the results of its assessment for CTS, in particular ship systems, are often not automated. As a result, the quality of decisions made to ensure the reliability indicators of such CTS significantly depends on the qualifications of the personnel operating the system [6,7,8].

Evolution in information processing leads to the actualization of the task of not only automating the process of assessing the reliability of elements and components of complex systems, but also to the transfer of part of the intellectual sphere of human activity to the sphere of automation of making and supporting management decisions in the field of ensuring the reliability of CTS.

The creation of intelligent decision support systems (IDSS), in the context of progress in the field of information systems and technologies, find significant application in solving complex, difficult to formalize problems, in particular, diagnosing the reliability of CTS. Distinctive features of problems that are difficult to formalize are the incomplete amount of initial data of the problem being solved, inaccuracy, heterogeneity, and significant computational complexity [9,10].

The purpose of the study is to ensure the reliability of CTS elements and components during operation based on the use of an intelligent decision support system for assessing their technical condition.

The objectives of the study are to develop a IDSS with insufficient information for assessing the technical characteristics of complex systems.

Analysis of the operating principle of the IDSS. Intelligent assessment of TC is a process that includes monitoring, diagnostics and, as a result, evaluation of the vehicle while simultaneously working with knowledge and large amounts of information.

This problem can be solved by using an expert decision support system. Decision support system is a computer system that allows the user to solve professional problems based on the use of databases, knowledge and models, by providing conclusions, recommendations, and assessments of possible alternative solutions to the problem. That is, IDSS helps the user solve a complex problem automatically [11].

In general, IDSS are information expert systems. Expert systems used to assess the reliability of CTS elements and assemblies are recommended to be built on the basis of artificial intelligence. This will make it possible to make management decisions in an automated mode, taking into account the specific tasks of monitoring and diagnosing the CTS.

The implementation of the IDSS should be based on the use of research results on the model of a specific operating CTS [5].

Previously developed mathematical models used to determine and evaluate the reliability indicators of CTS elements and assemblies, using the example of ship systems, were developed and presented in [5].

They make it possible to determine the probabilities and risks of failure of CTS elements and assemblies. Similar models can be used in the development of IDSS to assess the technical condition of complex systems.

Such systems solve problems: choosing the best solution from many possible ones - optimization; ordering possible solutions according to preferences - ranking. In both problems, the first and most fundamental point is the selection of a set of criteria on the basis of which alternative solutions are evaluated and compared.

Main part. A IDSS is proposed to evaluate the CTS TC. In such a system, in contrast to classical artificial intelligence systems, the theory of decision making is applied instead of attempts to "take into account uncertainty" using production rules of the form "IF.

For the practical implementation and operation of IDSS, it is necessary to link the developed models to an expert system containing calculated, experimental, and also data acquired by experts during the operation of the CTS. The block diagram of the developed IDSS (DSS, knowledge base) for assessing the technical condition of the CTS is shown in Fig. 1.

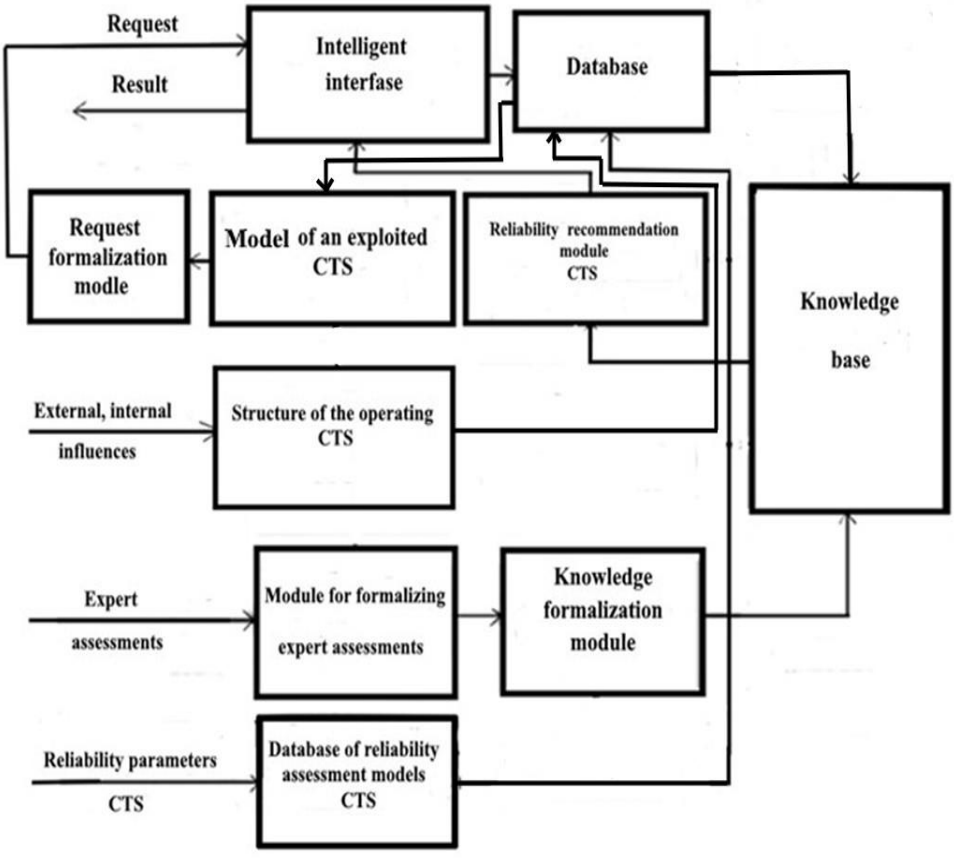


Fig.1. Block diagram of knowledge base, DSS for assessing the technical condition of CTS

When developing a IDSS, a ship's CTS, or more precisely a ship's power plant (SPP), was chosen as the object for assessing the reliability of the technical condition. Such a system is one of the main CTS out of almost hundreds of technical systems installed on the ship. Assessing the reliability of the SPP needs to take into account the fact that the CTS is characterized by a large number of diagnosed parameters that differ in information content and degree of accessibility, as well as specific and varied

operating conditions. In addition, the CTS is characterized by insufficient information about its technical condition.

The functioning of the developed DSS is based on an assessment of the risk of failure of elements and components of the CTS. Those. on criteria that reflect taking into account the specifics of the interaction of various elements and components, the correlation of changes in the values of their parameters under various emergency operating conditions of a complex system.

The developed IDSS (Fig. 1) evaluates the reliability of the system using a unified system of parameters of the elements and components of the control system.

IDSS cores are: database; a knowledge base with methods for calculating reliability indicators (probabilities and risks of failures) and a set of decision rules for selecting appropriate decision-making methods; intellectualization model for assessing the technical condition of CTS elements and components.

The basis for constructing an IDSS is the formulation of the decision-making problem in general form:

$$N = f(F, G, A, FR, SG, P, C, PC, NS),$$

where *F*– many failures of elements and components of the CTS;

G – many set goals (to ensure the reliability of the CTS);

A – many possible alternatives;

FR - multiple failure levels of elements and components of the CTS;

SG,P,C – set of characteristics, preferences, criteria for ensuring the reliability of elements and components of the CTS;

PC - many principles for coordinating the assessment of alternatives based on individual criteria; *NS*– necessary solution to the problem

Preference *F* – assessment of the usefulness of the method of achieving the goal. The assessment is specified without highlighting the characteristics by which it is made or the characteristics *SG*. The characteristics include the degree of achievement of the goal. To make the final choice of how to achieve the goal, it is necessary to formulate criteria *C*, the number of which is determined by the number of features. If multiple criteria are used in the IDSS, then it is necessary to apply the principles of *PC* coordination to agree on the assessment of alternatives for each criterion.

To support decision-making on assessments of the risk of CTS failures based on a priori and a posteriori data, as well as when searching for failed elements and system components in order to increase the efficiency of their operation, a method based on dynamic Bayesian trust networks (DBTN) is used [12,13]. The use of DBTN makes it possible to determine with great accuracy the elements and components of the CTS that are closest to the critical state and their failure.

The task is solved by using a constant system of polling all elements of the system at its various levels for a specific period of time. This allows, with the help of DBTN, to study extreme situations and accurately determine the critical values of the risk of failure of elements and components of the CTS.

The construction and study of the DBTN probability of loss of performance, assessment of the risk of failure of elements and components of the CTS was carried out using the GiNIe software product [14]. The decision support strategy used when searching for failures of elements and components of ship CTS consists of a number of stages (Fig. 2).

The implementation of the strategy in the IDSS scheme for assessing the technical condition of the CTS (Fig. 1) is ensured by targeted actions in accordance with the IDSS algorithm (Fig. 3) when searching for failures of elements and components based on assessments of the risk of failure of the diagnosed CTS.

At the initial stage, the numerical values of preliminary assessments of failures of elements and components of the CTS are determined using a diagnostic model based on DBTN. The input variables for the Bayesian diagnostic model are test results.

The model of the operating CTS in the intelligent system for assessing the risk of failure of system components (Fig. 1) in the form of DBTN can be written [5]:

$$< M, S, R, L >,$$

where M - is the set of elements. components;

S - many interelement, intercomponent connections;

R - many diagnostic assessments of the risk of failure of elements, components, interelement, intercomponent connections;

L - display of connections between the sets M, S and R, based on the diagnostic model of the CTS.

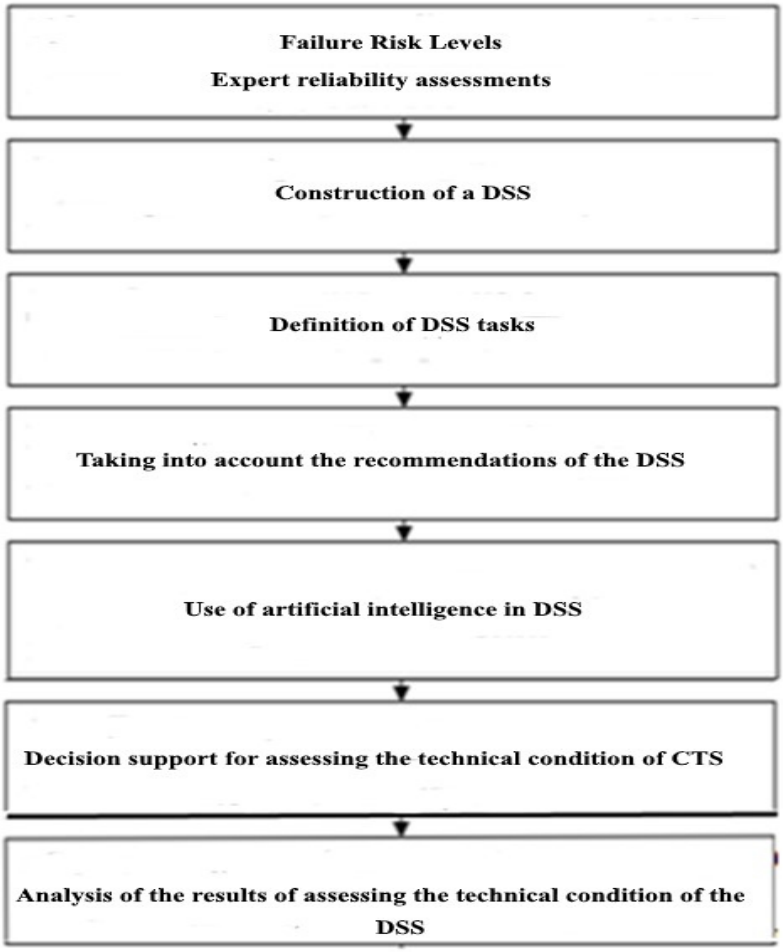


Fig. 2. Strategy for decision support when searching for failures in CTS

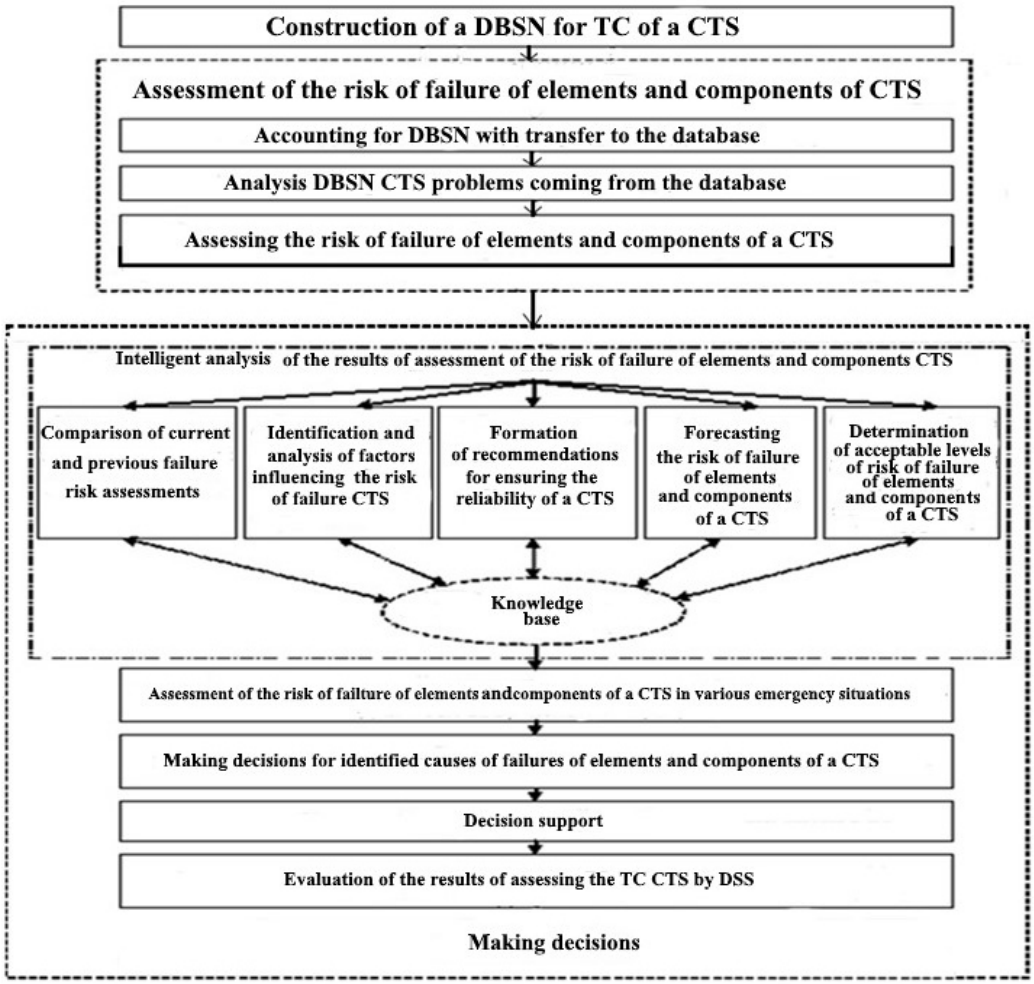


Fig. 3. IDSS algorithm when searching for failures of ship CTS

As a result of the functioning of the intelligent IDSS for vehicle assessment (using the example of a ship's CTS) in accordance with the algorithm shown in Fig. 3, using the SPP model in an intelligent system (Fig. 1) and DBTN , the dependences of the risk of failure are determined for different samples of failure probabilities of elements and components of systems serving the SPP (Fig. 4, Fig. 5)

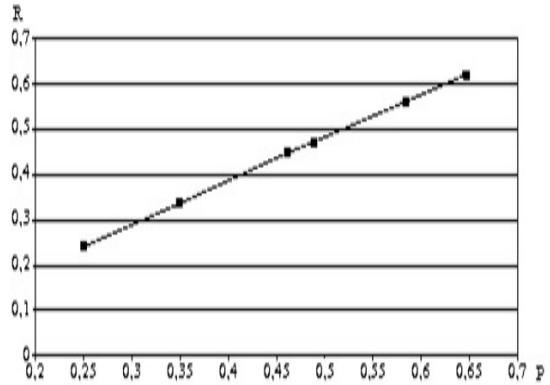


Fig. 4. Dependence of the risk of system failure on the probability of failure of elements of the SPP oil system

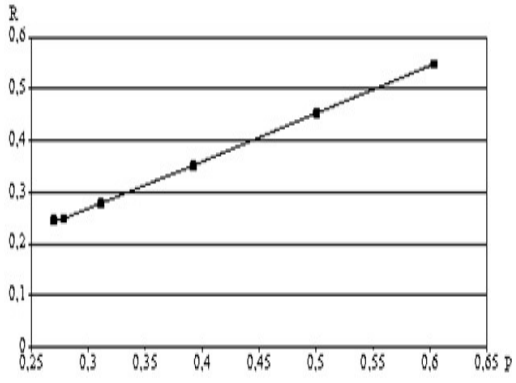


Fig. 5. Dependence of the risk of system failure on the probability of failure of elements of the SPP compressed air system

The problem-oriented knowledge base model is based on the following lists:

• elements. components affecting the trouble-free operation of the CTS;

• states in which the CTS may be in the process of failure-free operation of elements and system components;

• factors under the influence of which the current reliability of the CTS may change, systems transition to a state of failure with disruption of reliable operation;

• problem states into which the CTS can go under the influence of failures of elements and components.

The knowledge base can be presented in the form of a five-level hierarchical tree (Fig. 6).

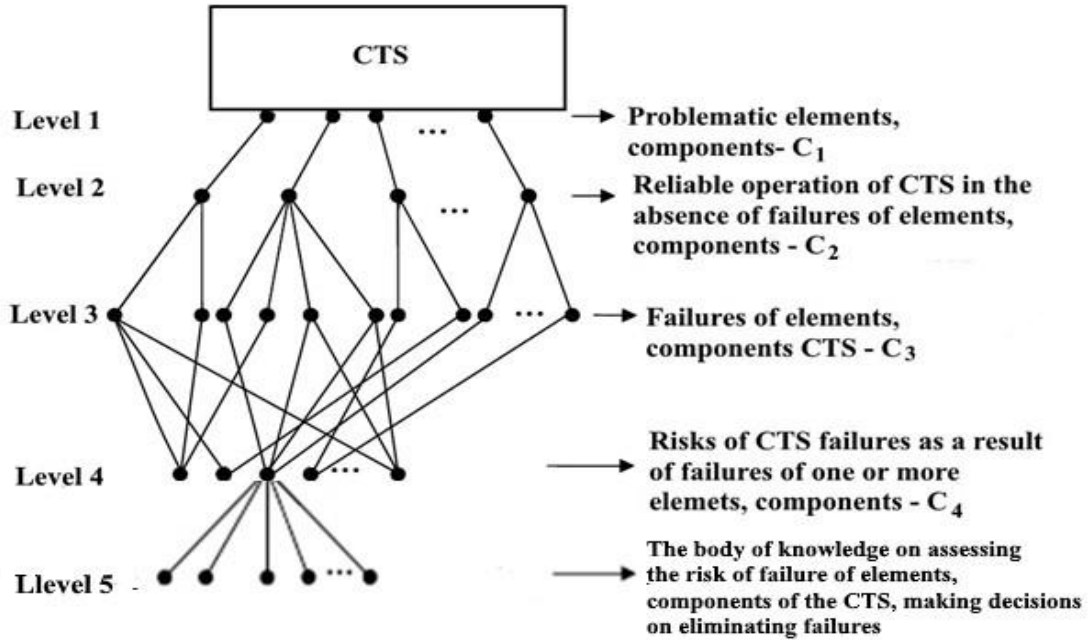


Fig. 6. Multi-level hierarchical structure of the knowledge base tree

Taking into account the hierarchical structure of the knowledge base allows you to quickly localize the cause of a defect or failure and reduce the time for diagnosing CTS.

The acquisition and addition of knowledge is carried out automatically during training and implementation of the expert system. Filling with knowledge is provided by an expert, as well as by adapting the knowledge base to changes in the subject area and the conditions of its functioning. This is implemented by replacing rules or information in the knowledge base of the IDSS.

Conclusions. The proposed decision support system contains: a knowledge base with methods for calculating reliability indicators (probabilities and risk of failures); results of determining the probabilities and risk of failures of elements and components of complex technical systems; intellectualization model for assessing the technical condition of elements and components. The proposed algorithm for the functioning of a decision support system implements the task of automating the process of assessing the technical condition of complex systems. The use of an intelligent decision support system for assessing the technical condition of complex systems makes it possible to establish the degree of risk of failure of elements and components of the CTS, which increases the efficiency of the systems. The use of the proposed decision support system for assessing the technical condition of complex systems will improve the reliability of operating systems with insufficient information about their technical condition.

References

1. Vychuzhanin V.V., Rudnichenko N.R., Sagova Z., Smieszek M., Cherniavskyi V.V. Analysis and structuring diagnostic large volume data of technical condition of complex equipment in transport. *IOP Conference Series: Materials Science and*

Engineering, Volume 776, 24th Slovak-Polish International Scientific Conference on Machine Modelling and Simulations - MMS 2019, 3-6 September 2019, Liptovský Ján, Slovakia. URL: https://doi.org/ 10.1088/1757-899X/776/1/012049
2. Vychuzhanin V.V., Rudnichenko N.R.Metod upravleniya riskami sudovykh slozhnykh tekhnicheskikh system. *Problemy tekhniky.* 2014. No.2. P.138-142.
3. ISO 13381-1:2015 Condition monitoring and diagnostics of machines – Prognostics – Part 1: General guidelines. Enter. 2015-03-01. 2015. 21 p.
4. Vychuzhanin V.V., Rudnichenko N.D. Metody informatsionnykh tekhnologiy v diagnostike sostoyaniya slozhnykh tekhnicheskikh sistem. Odesa: Ekologiya, 2019. 178 p.
5. Vychuzhanin A.V. Intelligent system for assessing and forecasting the risk of failure of components of a complex technical system. *Informatics and Mathematical Methods in Simulation*. 2022. Vol. 12. No. 3. P. 154-161. URL: https://doi.org/10.15276/imms.v12.no3.154
6. Zhang P., GaoCao Z., Dong L. Marine Systems and Equipment Prognostics and Health Management. *Systematic Review from Health Condition Monitoring to Maintenance Strategy. Machines.* 2022. No.10. P.72. URL: https://doi.org/10.3390/machines10020072
7. Zhang M., Montewka J., Manderbacka T., Kujala P., Hirdaris S. A Big Data Analytics Method for the Evaluation of Ship - Ship Collision Risk reflecting Hydrometeorological Conditions. *Reliability Engineering & System Safety.* 2021. V. 213. 107674. URL: https://doi.org/10.1016/j.ress.2021.107674
8. Chenguang Y., Jing N. Neural Network for Complex Systems: Theory and Applications. 2018. URL: https://doi.org/10.1155/2018/3141805
9. Phillips-Wren G. Intelligent Decision Support Systems. Innovations in Knowledge Management. 2018. URL: https://doi.org/ 10.1002/9781118522516.ch2
10. Ahmad A., Basir O. Hassanein K. Intelligent expert systems approach to layout decision analysis and design under uncertainty. Intelligent Decision Making: An AI-Based Approach. Berlin: Springer, 2008. P. 321–364.
11. Ahmad A., Basir O., Hassanein K. Intelligent expert systems approach to layout decision analysis and design under uncertainty. Intelligent Decision Making: An AI-Based Approach. Berlin: Springer, 2008. P. 321–364.
12. Jensen F.V. Bayesian Networks and Decision Graphs. Berlin: Springer, 2007. 457 p.
13. Wang C. R., Guan C. A Bayesian inference-based approach for performance prognostics towards uncertainty quantification and its applications on the marine diesel engine. *ISA Trans.* 2021. V.118, P.159–173.
14. Genie Timeline Professional. URL: https://zoolz.com/genie9/

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНКИ ТЕХНІЧНОГО СТАНУ СКЛАДНИХ СИСТЕМ

О.В. Вичужанін

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mail: v.v.vychuzhanin@op.edu.ua

Актуальність теми обумовлена необхідністю прийняття рішень щодо забезпечення надійності елементів і вузлів складних технічних систем при недостатній інформації про їх технічний стан. Проблема, що розв'язується, є напівструктурною та міждисциплінарною. Ефективність вирішення проблеми полягає у використанні інформаційних технологій та методів штучного інтелекту, зокрема експертних систем. Розглянуто переваги використання інформаційних технологій для автоматизації процесу прийняття рішень щодо оцінки поточного технічного стану складних систем. Розроблено інтелектуальну систему підтримки прийняття рішень, яка дозволяє оцінювати ризик відмови елементів і компонентів складних технічних систем з використанням елементів штучного інтелекту. Пропонована система підтримки прийняття рішень містить: базу даних; база знань з методами розрахунку показників надійності (ймовірності та ризиків відмов) і набір правил прийняття рішень для вибору відповідних методів прийняття рішень; результати визначення ймовірностей і ризиків відмов елементів і вузлів складних технічних систем з їх ранжуванням; модель інтелектуалізації для оцінки технічного стану елементів і вузлів. Запропонований алгоритм функціонування системи підтримки прийняття рішень реалізує завдання автоматизації процесу оцінки технічного стану складних систем. Використання запропонованої системи підтримки прийняття рішень для оцінки технічного стану складних систем дозволить підвищити надійність технічних систем з недостатньою інформацією про їх технічний стан.

Ключові слова: інформаційні технології, алгоритм, складні технічні системи, підтримка прийняття рішень, інтелектуальні системи, штучний інтелект, експертні системи, база знань, база даних, алгоритм, складні технічні системи, надійність, ризик відмови, судова енергетична установка

DOI 10.15276/imms.v13.no3-4.228
UDC 004.62

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 228-235

RESEARCH OF PROGRESSIVE TOOLS OF PARALLEL COMPUTATIONS WITH THE USE OF SIMD ARCHITECTURE

O.O. Zhulkovskyi[1], I.I. Zhulkovska[2], H.Ya. Vokhmianin[1],
O.D. Firsov[2], V.A. Riabovolenko[2]

[1]Dniprovsky State Technical University
Dniprobudivska str., 2, Kamianske city, 51918, Ukraine
e-mail: olalzh@ukr.net
[2]University of Customs and Finance,
Volodymyr Vernadskyi str., 2/4, Dnipro, 49000, Ukraine
e-mail: inivzh@gmail.com

The current stage of development of processes and technologies requires continuous improvement of computer hardware performance, efficient use of its resources, processing of large amounts of data and support of the growing requirements of modern information systems. When processing large amounts of data, it is often necessary to use additional effective solutions to speed up information processing in addition to parallel computing. One such approach is to use the SIMD mechanism. The concept of SIMD instructions is a progressive solution for speeding up computations in tasks with large amounts of data, due to the ability to perform one operation on several data simultaneously. The purpose of the study is to evaluate the effectiveness of using SIMD instructions to improve the performance of software code execution when processing large data sets compared to traditional software tools. The paper solves the following tasks: develop an algorithm for implementing the classical task of multiplying ultra-large (up to 36×10^6 bytes) square data matrices using the built-in Microsoft Visual Studio ISO/IEC C++20 <immintrin.h> library with SIMD technology to parallelise the program at the data level; study the performance of the developed algorithm when processing a significant amount of data compared to the traditional approach. By implementing a modified matrix multiplication algorithm using SIMD technology, it was possible to speed up the computation on a PC with an Intel Core i7-12700H processor by 4.8 times with a data volume of $\sim9\times10^6$ bytes. The obtained results will be taken into account in the development of application software, including for efficient computer models of technological processes and systems.

Keywords: SIMD, vector register, data-level parallelism, intrinsic function, computing acceleration, big data, computer modelling.

Introduction. A significant role in modern programming, especially in computer modeling, is the problem of computational efficiency and speed, which becomes notably prominent during large data processing. There is a need to apply, in addition to parallel computations, additional effective solutions to accelerate information processing. One such approach is the use of the SIMD mechanism (Single Instruction, Multiple Data).

The SIMD concept has long been present in the architecture of modern PCs and is used in processor technologies. It provides data-level parallelism, allowing one operation to be performed on multiple data simultaneously, significantly increasing program performance. Despite being an old concept, modern processors typically apply SIMD extensions to enhance parallel computation performance.

Literature review. The SIMD instruction is an element of classification according to M. Flynn's taxonomy for parallel processors, proposed in 1966 and later expanded in 1972 [1]. Modern PCs use this architecture in the form of integrating special instruction sets or command extensions to accelerate specific types of computations.

SIMD extensions are considered one of the significant features of modern general-purpose processors (GPPs), aimed at improving software performance with minimal hardware modifications [2].

Different processor manufacturers, such as Intel, AMD, etc., have their own Instruction Set Architecture (ISA) and SIMD microarchitectures. However, Intel has significantly expanded SIMD technologies from both hardware and software perspectives. In the context of microprocessor development, there is an increase in register bit-width from 64 to 512 bits and an increase in the number of vector registers from 8 to 32, providing more parallelism paths and reducing excessive data movement to cache memory [2].

SIMD vector extensions have become an integral part of high-performance processors. Various architectures, such as x86, ARM, MIPS, and PowerPC, have specific instruction sets and microarchitectures for SIMD vector extensions. Applying SIMD vectorization can significantly improve algorithm performance with minimal overhead on equipment. This is especially important for optimizing computational performance [3].

The «single instruction – multiple data» type of parallel processing (Fig. 1) represents a parallel computing technology where one instruction is executed over multiple data simultaneously [1-4].

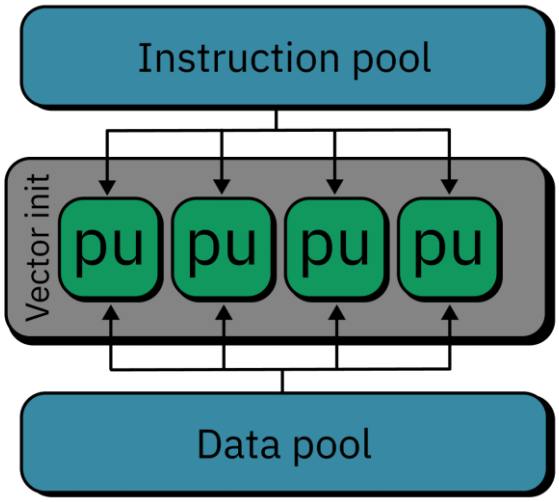


Fig. 1. SIMD architecture diagram

The Data pool is responsible for storing all processed data. The Instruction pool is responsible for storing executed instructions. The Vector unit is a key component of the SIMD architecture. It consists of several processing units (PU), each of which can process data in parallel. When a program runs on the SIMD architecture, the same instruction is sent from the instruction set to each processing device in the vector block. Each processing device then executes this instruction on different data from the set simultaneously. This allows SIMD to efficiently process large volumes of data, especially when one operation needs to be performed on each data element [1-4]. Accordingly, this technology finds its place in industries dominated by uniform operations, especially if they are applied to large volumes of data: graphics, signal processing, computer vision, computer modeling, etc.

A processor register used to store multiple data elements simultaneously in the form of a vector is called a vector register. Typically, vector elements represent a separate data value or component. Vector registers are part of SIMD hardware support, allowing the execution of a uniform operation over all vector elements simultaneously. They have a fixed width [5]. For example, a 128-bit vector register can store four float

data type values. Thus, the size of the vector register determines the number of data elements that can be stored in each register. Depending on the specific processor architecture, support for different data types, including integers, floating-point numbers, etc., is possible, and the number of elements can reach 4, 8, 16, or more. Examples of vector registers from Intel include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions) [2-4]. There are also NEON registers in some ARM processors [6].

SIMD technology is effective only in tasks where one operation can be applied to a large amount of data simultaneously. In other cases, its efficiency is either reduced or completely absent or negative. Among the disadvantages of SIMD, there is also a dependence on the architecture, as SIMD instructions may vary depending on the processor architecture, so a potential algorithm will work differently on different hardware systems [2, 7].

Recent studies have proposed significant improvements to multimedia applications aimed at increasing the performance, versatility, and programmability of computing cores. This involves the implementation of a massively parallel matrix SIMD core (CAMX) based on Content Addressable Memory, designed to work as an accelerator for processor cores. Notably, the study confirms the efficiency of CAMX with a detailed analysis of its operation during AES encryption [8].

Research in the field of graph computations using matrices also highlights the use of SIMD extensions on multi-core processors for efficient execution of graph algorithms. In particular, the graph algorithm compiler is adapted for the use of SIMD extensions on processors, leading to a significant acceleration of the naive multi-threaded implementation [9, 10].

To address the problem of sorting arrays containing a large amount of data, a parallel sorting implementation for MIPS processors is possible, based on concrete sorting networks and SIMD instructions [11].

Research Objective. The aim of this study is to evaluate the efficiency of using SIMD instructions to enhance the performance of programs during the processing of large data arrays compared to traditional software tools.

To achieve the set goal, the following tasks were formulated: Development of an algorithm for implementing the classic problem of multiplying ultra-large square data matrices using SIMD technology; Investigation of the performance of the developed algorithm with a significant amount of processed data compared to the traditional approach; Analysis of the obtained results and the development of a concept for the effective use of modern computing systems and tools to increase the productivity of computer applications.

Main Part. This work examines the evaluation of the efficiency of using SIMD instructions to accelerate computations in tasks of processing ultra-large data arrays. The research involves the development of a modified algorithm for solving the classic problem of processing large data arrays using SIMD instructions and analyzing the efficiency of applying this method compared to the traditional data processing approach.

One of the modern programming languages that provides and supports SIMD instructions is C++. Here, this technology is used thanks to compiler specifications and extensions, as well as through the use of specialized libraries.

For example, to use various sets of SIMD instructions from Intel, such as SSE, AVX, AVX2, AVX-512, etc., in C++, one can use special data types: __m128, __m256, __m512, etc. They represent vectors with 4, 8, or 16 elements of the corresponding type [7].

At the same time, the Intel Intrinsics library provides special functions for generating and using SIMD instructions [7]:

– The _mm_add_ps function is an intrinsic function (a special low-level function that provides access to processor instructions) for performing addition operations on several floating-point values in a vector register with a specified precision;

– The _mm_mul_pd function is also intrinsic, designed to perform multiplication operations on several double-precision floating-point values in a vector register.

In addition to the mentioned functions, there are many others, including subtraction, division, comparison, data loading and saving, bitwise arithmetic, element permutations, etc. Most of them can also define floating-point precision: single or double.

To use the listed instructions, the built-in library <immintrin.h> is used. It includes all Intel SIMD intrinsics, providing access to them. Also, for various SIMD extensions, different libraries are used. For example, for SSE, you should connect the header file <xmmintrin.h>, MMX is provided after connecting <mmintrin.h>, etc. But connecting one of the header files that provide access to the use of various extensions automatically connects all previous ones.

Thus, the variety of functions allows for the effective use of SIMD technology for various tasks and operations, leading to a significant increase in the productivity of computational tasks that support parallel data processing [7].

To maximize the power of processors with minimal development costs, it is advisable to use the NSIMD library, which abstracts SIMD programming and provides the following main paradigms [12]:

– Imperative programming provided by the NSIMD core and supports numerous CPU/SIMD extensions;

– Expression templates provided by a separate module that supports all architectures from the NSIMD core.

To achieve maximum performance, NSIMD uses optimized built-in compiler functions. Therefore, using any basic compiler can provide a SIMD abstraction library without significant costs. NSIMD supports work in all modern C++ programming language standards [12].

Another example of SIMD extension in C++ is the OpenMP standard for parallel programming, which supports the simd directive, which can be used to vectorize loops thanks to the #pragma omp simd construct. In this case, the compiler can ignore vector dependencies, considering the intention to execute several iterations simultaneously [13].

The mentioned ways of using SIMD technology allow for accelerating calculations by performing one operation on several data simultaneously.

For research purposes, an algorithm was developed to implement the classic problem of multiplying ultra-large square data matrices using the built-in Microsoft Visual Studio ISO/IEC C++20 <immintrin.h> library with SIMD technology for data-level program parallelization; an analysis of the performance of the developed algorithm was carried out with a significant amount of processed data compared to the traditional data processing approach.

For the experiments, the following PC infrastructure was used: Intel Core i7-12700H (14 cores, 2.3 GHz / 4.7 GHz); Goodram DDR4 (16 GB) × 2 = 32 GB; Microsoft Windows 10.

Program testing was conducted for matrices of size 100–3000, filled with random float type values (4 bytes) using a 128-bit register. Using wider registers may not be supported by some processors and requires more program resources. The obtained results are presented in Table 1.

Table 1

Computational Experiment Results

Matrix Dimension	Data Size, bytes	Execution Time, s		Acceleration a=s1/s2
		Traditional Algorithm (s1)	SIMD Algorithm (s2)	
100	4×10^4	$3{,}27\times10^{-4}$	$1{,}3\times10^{-4}$	2,53
500	10^6	$7{,}2\times10^{-2}$	$1{,}7\times10^{-2}$	4,24
1000	4×10^6	0,854	0,195	4,38
1500	9×10^6	2,89	0,604	4,78
2000	16×10^6	10,18	2,88	3,53
2250	$20{,}25\times10^6$	19,09	6,14	3,11
2500	25×10^6	30,96	8,97	3,45
2750	$30{,}25\times10^6$	48	14,55	3,30
3000	36×10^6	79,64	24,53	3,25

With the increase in matrix size, and therefore the volume of processed data, there is a natural increase in their processing time, regardless of the applied calculation algorithm. The use of SIMD technology has significantly accelerated the execution of calculations in all test cases and, especially, with a matrix dimension of 1500×1500 elements (data size 9×10^6 bytes).

Figure 2 shows that with an increase in matrix size in the range of 100–3000 float type elements, the computational data processing time increases significantly – from 33 ms to 80 s with the traditional (STD) algorithm and from 13 ms to 24.5 s with the SIMD algorithm.

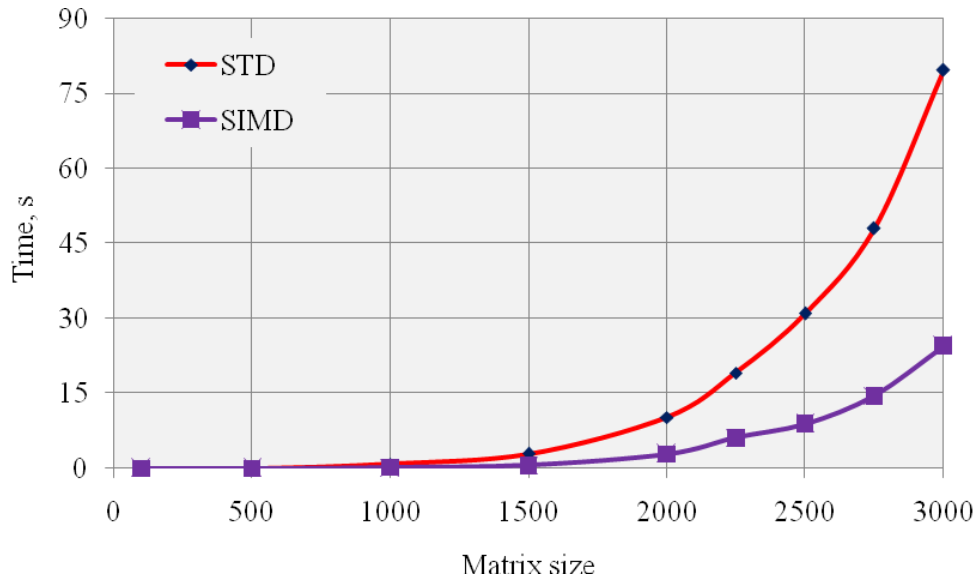


Fig. 2. Dependence of the implementation time of the compared algorithms on the dimensionality of the data matrices.

The acceleration of calculations when using SIMD technology compared to traditional data processing (Fig. 3) is between 2.53–4.78 and does not depend on the volume of processed data. The highest acceleration (~4.8), as already mentioned, is demonstrated by the modified algorithm with a matrix dimensionality of 1500 elements (~9×10^6 bytes), which should be taken into account during the development of application software.

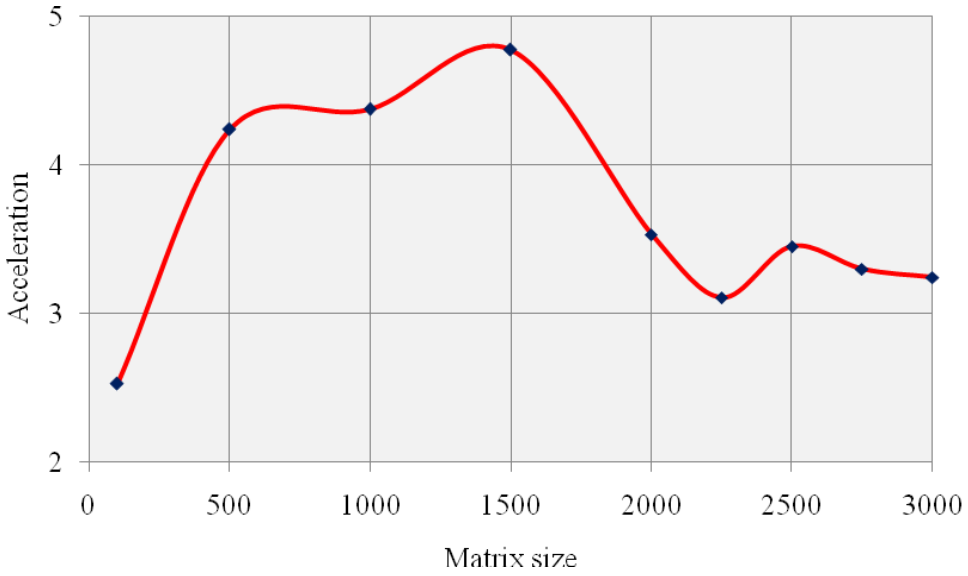


Fig. 3. Dependence of calculation acceleration due to the application of SIMD technology on the dimensionality of the data matrices.

Thus, the research has proven the effectiveness of using SIMD technology for solving tasks related to the processing of large volumes of data. The obtained data correspond with the results of known studies [3, 5] on the issue of enhancing the productivity of computer calculations using SIMD technology.

The use of the findings in conjunction with other alternative software tools to enhance computational productivity [14, 15] will contribute to the development of efficient computer models of technological processes and systems [16].

Conclusions. An algorithm has been developed to implement the classic problem of multiplying ultra-large square data matrices using SIMD technology. The performance of the developed algorithm was investigated with a significant amount of processed data (up to 36×10^6 bytes) compared to the traditional approach. The effectiveness of using advanced computing systems and SIMD-type tools to increase the productivity of application computer programs during the processing of large data volumes has been proven.

It has been established that the acceleration of calculations on a PC with an Intel Core i7-12700H processor, due to the application of SIMD technology compared to traditional data processing, is between 2.53–4.78 and does not depend on the volume of processed data. The highest acceleration (~4.8) is achieved with a matrix dimensionality of 1500 elements (~9×10^6 bytes), which should be taken into account during the development of application software, including for efficient computer models of technological processes and systems.

References

1. Flynn M. J. Some Computer Organizations and Their Effectiveness. *IEEE Transactions on Computers*. 1972. Vol. C-21, № 9. P. 948-960. URL: https://doi.org/10.1109/TC.1972.5009071
2. Amiri H., Shahbahrami A. SIMD programming using Intel vector extensions. *Journal of Parallel and Distributed Computing*. 2020. Vol. 135. P. 83-100. URL: https://doi.org/10.1016/j.jpdc.2019.09.012
3. Xie C., Wu H. Zhou J. Vectorization Programming Based on HR DSP Using. *MDPI Journals Awarded Impact Factor*. 2023. Vol. 12, № 13. URL: https://doi.org/10.3390/electronics12132922
4. Lee S., Kye H. Efficient MIP volume rendering via fast SIMD interpolation and memory access reordering. *Multimedia Tools and Applications*. 2023. Vol. 82.

URL: https://doi.org/10.1007/s11042-022-13732-z
5. Chen Yi., Mendis C., Carbin M., Amarasinghe S. VeGen: a vectorizer generator for SIMD and beyond. *Proceedings of the 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*. 2021. P. 902-914.
URL: https://doi.org/10.1145/3445814.3446692
6. Lindoso A., Garcia-Valderas M., Entrena L. Analysis of neutron sensitivity and data-flow error detection in ARM microprocessors using NEON SIMD extensions. *Microelectronics Reliability*. 2019. Vol. 100-101. URL: https://doi.org/10.1016/j.microrel.2019.06.038
7. Compiler intrinsics. URL: https://learn.microsoft.com/en-us/cpp/intrinsics
8. Kageyama K., Arai S., Hamano H., Kong X., Koide T., Kumaki T. Implementation of parallel AES Processing with CAM-based Massive-parallel SIMD Matrix Core. *2022 5th World Symposium on Communication Engineering (WSCE)*. 2022. Vol. 5.
URL: https://doi.org/10.1109/WSCE56210.2022.9916049
9. Zheng R., Pai S. Efficient Execution of Graph Algorithms on CPU with SIMD Extensions. *2021 IEEE/ACM International Symposium on Code Generation and Optimization (CGO)*. 2021. URL: https://doi.org/10.1109/CGO51591.2021.9370326
10. Mehrafsa A., Chester S., Thomo A. Vectorising k-Truss Decomposition for Simple Multi-Core and SIMD Acceleration. *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*. 2022. Vol. 13.
URL: https://doi.org/10.1109/IISA56318.2022.9904350
11. Brankovic S., Markovic A., Simic D., Rikalo A. Improving performance of sorting small arrays on MIPS CPUs using bitonic sort and SIMD instructions. *2019 27th Telecommunications Forum (TELFOR)*. 2020. Vol. 27.
URL: https://doi.org/10.1109/TELFOR48224.2019.8971325
12. NSIMD Documentation. URL: https://github.com/agenium-scale/nsimd
13. SIMD Extension. URL: https://learn.microsoft.com/en-us/cpp/parallel/openmp/openmp-simd
14. Zhulkovskyi O.O. Evaluating the effectiveness of the implementation of computational algorithms using the OpenMP standard for parallelizing programs. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, №4. P. 268-277. URL: https://doi.org/10.15276/imms.v11.no4.268
15. Zhulkovskyi O. O. Evaluation of the efficiency of the implementation of parallel computational algorithms using the <thread> library in C++. *Computer Systems and Information Technologies*. 2022. №3. P. 49-55.
URL: https://doi.org/10.31891/csit-2022-3-6
16. Zhulkovskii O. A., Panteikov S. P., Zhulkovskaya I. I. Information-Modeling Forecasting System for Thermal Mode of Top Converter Lance. *Steel in Translation*. 2022. Vol. 52, №5. P. 495-502. URL: https://doi.org/10.3103/s0967091222050138

ДОСЛІДЖЕННЯ ПРОГРЕСИВНИХ ЗАСОБІВ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ІЗ ЗАСТОСУВАННЯМ SIMD АРХІТЕКТУРИ

О.О. Жульковський[1], І.І. Жульковська[2], Г.Я. Вохмянін[1],
О.Д. Фірсов[2], В.А. Рябоволенко[2]

[1]Дніпровський державний технічний університет
2 Дніпробудівська вул., Кам'янське, 51918, Україна
e-mail: olalzh@ukr.net
[2]Університет митної справи та фінансів
2/4, Володимира Вернадського вул., Дніпро, 49000, Україна
e-mail: inivzh@gmail.com

Сучасний етап розвитку процесів та технологій потребує постійного підвищення продуктивності комп'ютерної техніки, ефективного використання її ресурсів, обробки великих обсягів даних та підтримки зростаючих вимог сучасних інформаційних систем. Під час обробки великих обсягів даних часто виникає необхідність застосування, окрім паралельних обчислень, додаткових ефективних рішень для прискорення обробки інформації. Одним з таких підходів є використання механізму SIMD. Концепція SIMD-інструкцій є прогресивним рішенням для пришвидшення обчислень у задачах з великим обсягом даних, завдяки можливості виконувати одну операцію над декількома даними одночасно. Метою дослідження є оцінка ефективності використання SIMD-інструкцій для підвищення продуктивності виконання програмного коду під час обробки великих масивів даних у порівнянні з традиційними програмними засобами. В роботі вирішені наступні задачі: розроблено алгоритм реалізації класичної задачі перемноження надвеликих (до 36×10^6 байт) квадратних матриць даних із використанням вбудованої бібліотеки Microsoft Visual Studio ISO/IEC C++20 <immintrin.h> з технологією SIMD для розпаралелювання програми на рівні даних; досліджено продуктивність виконання розробленого алгоритму при значній кількості оброблюваних даних у порівнянні з традиційним підходом. розроблено алгоритм реалізації класичної задачі перемноження надвеликих квадратних матриць даних із використанням; виконано аналіз продуктивності розробленого алгоритму при значній кількості оброблюваних даних у порівнянні з традиційним підходом до обробки даних Тестування програмного забезпечення проводилось для матриць розмірністю 100–3000, заповнених випадковими значеннями типу float (4 байти) із використанням 128-бітного регістру SIMD-архітектури. За рахунок впровадження модифікованого алгоритму перемноження матриць з використанням технології SIMD вдалося пришвидшити виконання обчислень на PC з процесором Intel Core i7-12700H у 4,8 рази при обсягах оброблюваних даних ~9×10^6 байт. Отримані результати будуть враховуватися під час розроблення прикладного програмного забезпечення, у тому числі для ефективних комп'ютерних моделей технологічних процесів та систем.

Ключові слова: SIMD, векторний регістр, паралелізм на рівні даних, інтринзична функція, пришвидшення обчислень, великі дані, комп'ютерне моделювання

DOI 10.15276/imms.v13.no3-4.236
УДК 004.056:351.861

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 236-242

МЕТОДИКА РІШЕННЯ ЗАДАЧ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ

В.В. Білозерський, О.Ю. Лебедєва, Н.П. Волкова, В.О. Назаров

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mails: o.y.lebedieva@op.edu.ua, volkova.n.p@op.edu.ua tasknavigator@gmail.com

Розроблено методику розв'язання задач із захисту інформації. Кібербезпека є однією з найважливіших проблем сучасного світу. Зростаюче використання цифрових технологій у всіх сферах життя робить кіберпростір все більш привабливим для кіберзлочинців. Захист інформаційних систем – одне з найважливіших завдань будь-якої служби безпеки будь-якої організації та будь-якого підприємства. Щоб протистояти цій загрозі, необхідно розробляти ефективні методи захисту інформації. В роботі розглянуті такі інструменти як відкритий стандарт для оцінки серйозності вразливостей безпеки комп'ютерної системи CVSS та база даних загальновідомих вразливостей інформаційної безпеки CVE. Є доцільним використання цих інструментів для створення списку ефективних сучасних атак. Крім цього ще необхідно визначитися з наявними інструментами захисту комп'ютерних систем організації. Кібербезпека спирається на різні математичні апарати, одним із таких є теорія ігор. Теорія ігор є одним із інструментів, які можуть бути використані для підвищення рівня кібербезпеки. В роботі використовуються матричні ігри двох гравців. В якості гравців виступають зловмисник, який атакує комп'ютерну систему якоїсь організації та представник організації, що відповідає за забезпечення захисту інформації. Теорія ігор дозволяє представити завдання захисту комп'ютерної системи в математичному вигляді, що дозволяє скористатися встановленими критеріями знаходження оптимальних стратегій захисту, дотримуючись яких адміністратор здатний усунути, або принаймні звести до мінімуму збитки інформації, що завдається зловмисником. Знаходження оптимальних чистих стратегій пов'язано з пошуком сідлової точки. Не кожна матрична гра має оптимальну чисту стратегію. Якщо матрична гра має сідлову точку, то гра має рішення в чистих стратегіях і дослідження гри закінчується знаходженням цієї точки та відповідної пари чистих стратегій гравців. В протилежному випадку застосовують змішані стратегії. Для пошуку змішаних стратегій пропонується використовувати метод Брауна-Робінсон.

Ключові слова: захист інформаційних систем, теорія ігор, матрична гра, метод Брауна-Робінсон.

Вступ. Комп'ютерні системи в наш час стають найпоширенішим ресурсом, на якому зберігається найрізноманітніша інформація. Підключення цих систем до мережі Інтернет призводить до того, що інформація, що зберігається, стає об'єктом нападу найрізноманітніших зловмисників, від окремих хакерів, що горять бажанням «пробити» захист ресурсу, до організованих злочинних спільнот, а також розвідувальних і військових служб різних держав.

Актуальність теми дослідження обумовлена постійним зростанням загроз кібербезпеці. Комп'ютерні системи багатьох підприємств часто стають об'єктами, куди спрямовані помисли зловмисників. Через несанкціонований доступ зловмисник може викрасти інформацію, а за допомогою комп'ютерної атаки або знищити її, або тимчасово обмежити доступ до неї. У будь-якому разі підприємства зазнають як фінансових втрат, так і моральних, як, наприклад, падіння рівня довіри до банків, якщо вони стали жертвами атаки хакерів.

Захист інформаційних систем – одне з найважливіших завдань будь-якої служби безпеки будь-якої організації та будь-якого підприємства.

Кіберзлочинці розробляють все більш складні методи атак, а кіберзахисники повинні постійно вдосконалювати свої методи захисту. Теорія ігор може стати цінним інструментом для вирішення цієї проблеми.

Мета та задачі роботи. Метою роботи є розробка методики рішення задач із захисту інформації шляхом використання теорії ігор.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- аналіз існуючих атак зловмисників та засобів захисту;
- розробка методики рішення задач із захисту інформації;
- розробка програмного додатку що реалізує розроблену методику.

Основна частина. Виявлення CVSS (Common Vulnerability Scoring System) – це відкритий стандарт для оцінки серйозності вразливостей безпеки комп'ютерної системи. Він був розроблений спільно групою експертів у галузі безпеки та впроваджений у 2005 році [1]. CVSS використовується для оцінки вразливостей за двома основними критеріями:

- вплив – виявлення потенційного впливу, який може мати вразливість на систему;
- експлуатація – оцінка того, наскільки легко може бути експлуатована вразливість.

CVSS оцінює вразливості за шкалою від 0 до 10, де 10 – найсерйозніша вразливість. Оцінки CVSS використовуються для розміщення пріоритетів на відповіді на вразливості та визначення того, які вразливості є найнебезпечнішими.

CVSS використовується багатьма організаціями, в тому числі уряди, підприємства та некомерційні організації. Він також використовується багатьма продуктами та послугами безпеки для оцінки вразливостей. CVSS постійно оновлюється, щоб враховувати нові загрози та можливості. Остання версія, CVSS 3.1, була опублікована в 2020 році.

CVE (Common Vulnerabilities and Exposures) – це база даних загальновідомих вразливостей інформаційної безпеки [2]. Кожній уразливості присвоюється унікальний ідентифікатор, який складається з року виявлення вразливості та послідовного номеру. CVE-номери присвоюються Центром з оцінки та розробки безпеки (CERT) при Національному інституті стандартів і технологій (NIST). Наприклад, уразливість, виявлена в 2023 році, буде мати ідентифікатор CVE-2023-0001.

CVE-номери використовуються для ідентифікації вразливостей безпеки в різних продуктах і системах, в тому числі програмне забезпечення, апаратне забезпечення та мережі. Вони використовуються розробниками програмного забезпечення, виробниками обладнання та організаціями з безпеки для спілкування про вразливості та розробки методів усунення. CVE-номери є важливим інструментом для забезпечення безпеки інформаційних систем. Вони допомагають організувати вразливості, зробити їх зрозумілими та сприяти їх усунення.

National Vulnerability Database (NVD) надає оцінки CVSS для всіх опублікованих записів у CVE.

Наприклад, якщо в якості комп'ютерної системи взяти операційну систему Windows 11, то згідно з CVE можна на даний час визначити такі категорії вразливостей:

- виконання довільного коду (Execute code);
- ескалація привілеїв (Privilege Escalation, Gain Privilege);
- відмова в обслуговуванні (Denial of Service);
- витік інформації (Information Leak).

Кожна категорія має певну кількість вразливостей.

Наприклад, вразливість CVE-2023-21554 **(**Windows Message Queuing Remote Code Execution Vulnerability, або віддалене виконання коду через чергу повідомлень Windows) виникає через помилку в обробці запитів на створення черг. Вразливість класифікується як критична, CVSS оцінюється в 9,8 балів. Вона може бути скомпрометована віддалено, тобто зловмиснику не потрібно мати фізичний доступ до комп'ютера.

Наприклад, вразливість CVE-2023-36028 (Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability або уразливість віддаленого виконання коду в захищеному розширюваному протоколі автентифікації від Microsoft) – це критична вразливість віддаленого виконання коду, яка існує в PEAP. Вразливість виникає через помилку в обробці запитів на аутентифікацію. Вразливість класифікується як критична, тобто CVSS оцінюється в 9,8. Може бути скомпрометована віддалено.

Наприклад, вразливість CVE-2023-21823 (Microsoft Graphics Component Denial of Service Vulnerability або відмова в обслуговуванні в графічному компоненті Microsoft) виникає через помилку в обробці повідомлень про помилки. Вразливість класифікується як критична, CVSS оцінюється також в 9.8. Вона може бути також скомпрометована віддалено, зловмиснику не потрібно мати фізичний доступ до комп'ютера.

В якості атак, ми пропонуємо розглянути всі вразливості з вказаних категорій, які мають високу оцінку CVSS. Аналіз показав що вони є найбільш поширеними та є максимально застосовуваними. Деякі з них є модифікаціями вразливостей попередніх років. Також є велика ймовірність того що деякі нові вразливості будуть модифіковані у майбутньому, так як нові вразливості є дуже гарною базою для цього.

Традиційний захисний механізм включає брандмауери, систему виявлення вторгнення (IDS) та антивірусні програми. Деякі з цих стратегій захисту розроблені лише для певних загроз.

В результаті, придбання та встановлення різноманітних засобів захисту інформаційного комп'ютерного ресурсу, може призвести до матеріальних витрат, потребує наявності інструкцій щодо ефективного їх використання. Необхідно розробити для системного адміністратора, служби безпеки комп'ютерної мережі оптимальну стратегію забезпечення захисту інформації, що зберігається.

Для вибору засобу ефективного захисту від різноманітних комп'ютерних атак можна використовувати методи теорії ігор. Метою теорії ігор є вироблення природних уявлень про оптимальність ситуацій і стратегій гравців, передбачення їх існування у грі та зазначення способу їх знаходження та перерахування [3].

Одним з важливих класів антагоністичних ігор є матричні ігри, які можуть бути використані для моделювання та аналізу конфліктних ситуацій [3]. Матриця гри – це інструмент, який представляє вибір гравців та їхні можливі варіанти дій (стратегії). Кожен гравець має свої власні стратегії, і результат гри залежить від комбінацій вибору кожного з учасників. Така концепція дозволяє аналізувати різноманітні сценарії та прогнозувати оптимальні стратегії для кожного гравця.

Основними елементами матричних ігор є правила гри, гравці, стратегії, виграші та втрати. Гравці приймають рішення, обираючи свої стратегії, і отримують виграш або втрату в залежності від вибору інших учасників. Задача теорії ігор – розробити моделі та аналізувати ситуації, де раціональні гравці вибирають стратегії для максимізації свого виграшу.

Зацікавлені сторони в грі називаються гравцями. Гравцем прийнято вважати одного учасника або групу учасників гри, які мають одні спільні для них інтереси, що не збігаються з інтересами інших груп.

В роботі використовувались матричні ігри двох гравців. В якості гравців ми використовували зловмисника, який атакує комп'ютерну систему якоїсь організації та представника організації, що відповідає за забезпечення захисту інформації (адміністратор безпеки).

Правила чи умови гри визначають можливі поведінки, вибір та ходи гравців на будь-якому етапі розвитку гри. Зробити вибір гравцеві, це означає зупинитися на одній із його можливостей поведінки. Потім гравець здійснює цей вибір за допомогою ходів.

Кожен гравець на певному етапі гри робить хід згідно зробленого вибору. Інший гравець, знаючи чи не знаючи про вибір першого гравця, також робить хід. Кожен із гравців намагається врахувати інформацію про минулий розвиток гри, якщо така можливість дозволяється правилами гри.

Будь-яка можлива для гравця дія (в рамках заданих правил гри) називається його стратегією. У разі конфлікту кожен гравець вибирає свою стратегію, у результаті складається набір стратегій, званий ситуацією. Стратегія в теорії ігор означає певний закінчений план дій гравця, що показує, як треба діяти йому у всіх можливих випадках розвитку гри. В якості стратегій зловмисника, або гравця А, використовуємо атаки на комп'ютерну систему організації, в якості стратегій сторони захисту, або гравця В, існуючі засоби захисту в організації.

Зацікавленість гравців у ситуації відображається в тому, що кожному гравцю в кожній ситуації приписується число, що виражає ступінь задоволення його інтересів у цій ситуації та називається його виграшем у ній. Як стратегії зловмисника будемо розуміти рядки матриці гри, а як стратегії адміністратора безпеки – її стовпці. На перетині рядка і стовпця в матриці ставиться виграш зловмисника (гравця А).

Вважатимемо, що зловмисник захоплений бажанням завдати якомога більшої шкоди комп'ютерній системі, що атакується. При такому припущенні виграш зловмисника дорівнюватиме програшу адміністратора безпеки і в цій ситуації використовується матриця гри для гри двох осіб з нульовою сумою.

Виграш зловмисника можна оцінити заподіяною матеріальною шкодою та ймовірністю реалізації атак зловмисника за обраної стратегії. Імовірність реалізації атак може бути визначена за результатами статистичних досліджень. Якщо ймовірності атак невідомі, можна припустити, що вони рівноймовірні.

У теорії ігор сідлова точка гри – це ситуація, в якій гравець не може поліпшити свій результат, змінивши свою стратегію, якщо інший гравець також дотримується своєї стратегії. Іншими словами, сідлова точка гри – це ситуація, в якій кожен гравець досягає найкращого можливого результату, беручи до уваги стратегію іншого гравця.

Сідлові точки мають важливе значення в теорії ігор, оскільки вони можуть допомогти гравцям знайти оптимальні стратегії.

Оптимальною називається стратегія, яка при багаторазово повторюваній грі гарантує гравцеві максимально можливий середній виграш (або еквівалентно мінімально можливий середній програш). Вибір оптимальної стратегії базується на принципі, який передбачає, що обидва гравці розумні в однаковому ступені та поведінка кожного з них спрямована на протидію противнику в досягненні його мети.

Теорія ігор дозволяє представити завдання захисту комп'ютерної системи в математичному вигляді, що дозволяє скористатися розробленими критеріями знаходження оптимальних стратегій захисту, дотримуючись яких адміністратор здатний усунути, або принаймні звести до мінімуму збитки інформації, що завдається зловмисникам.

Дослідження матричної гри починається з знаходження її сідлової точки у чистих стратегіях. Потенційно знаходження сідлової точки може бути корисно для кібербезпеки з кількох причин.

- можуть вказувати на потенційні вразливості в системі безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може отримати доступ до конфіденційних даних, це може вказувати на те, що система безпеки невідповідно захищена.
- можуть бути використані для розробки нових стратегій безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може отримати доступ до системи, але не може її повністю контролювати, це може вказувати на те, що атака може бути відбита, якщо будуть використані правильні заходи.
- можуть бути використані для оцінки ефективності існуючих стратегій безпеки. Наприклад, якщо сідлова точка знаходиться в точці, де атакуючий може легко отримати доступ до системи, це може вказувати на те, що існуючі заходи безпеки недостатньо ефективні.

Не кожна матрична гра має оптимальну чисту стратегію. Якщо матрична гра має рішення в чистих стратегіях, тобто для даної гри існує сідлова точка, то дослідження гри закінчується знаходженням даної сідлової точки та відповідних чистих стратегій гравців. Якщо ж гра повторюється багато разів, то кожен з гравців, з одного боку, отримує інформацію про попередні ходи супротивника, а з іншого боку, хоче приховати від супротивника свої наміри в майбутніх ходах. Кожен гравець може змінювати ймовірність застосування своїх чистих стратегій таким чином, щоб максимально збільшити свій середній виграш і на цьому шляху отримувати оптимальні стратегії. Така ідея призвела до поняття змішаної стратегії.

Змішаною стратегією гравця називається повний набір ймовірностей застосування його чистих стратегій. Для пошуку змішаних стратегій пропонується використовувати метод Брауна-Робінсон.

Алгоритм методу Брауна-Робінсон для гри з двома гравцями виглядає наступним чином:

- гравці обирають довільні змішані стратегії;
- гравці грають одну гру з обраними стратегіями;
- кожен гравець розраховує свій очікуваний виграш у цій грі;
- кожен гравець коригує свою стратегію таким чином, щоб збільшити свій очікуваний виграш.
- повторюються другий та останній кроки до досягнення бажаної точності.

В роботі запропонована методика для вирішення задач із захисту інформації, яка складається з наступних кроків:

Крок 1. Визначення стратегій зловмисника, а саме аналіз поширених вразливостей та ризиків.

Крок 2. Визначення засобів захисту. Цей крок являє собою відповідь на проаналізовані загрози, які можуть спричинити збитки.

Крок 3. Створення таблиці кореляції стратегій. Для кожного такого аналізу повинна бути створена таблиця, що показує кореляцію між стратегіями захисту та атаки.

Крок 4. Пошук величини збитків. Цей крок відповідає за розрахунок відповідних збитків, який повинен проводити адміністратор.

Крок 5. Визначення сідлової точки, та при її наявності оптимальних стратегій. Шляхом знаходження сідлової точки, при наявних результатах можливих атак, можна визначити оптимальні стратегії, які вплинуть на вибір захищаючої сторони.

Крок 6. Якщо сідлова точка не знайдена, визначення змішаних стратегій. Визначення змішаних стратегій виконується за допомогою методу Брауна-Робінсон.

Було розроблено програмний продукт, який реалізує запропоновану методику для вирішення задач із захисту інформації (рис. 1).

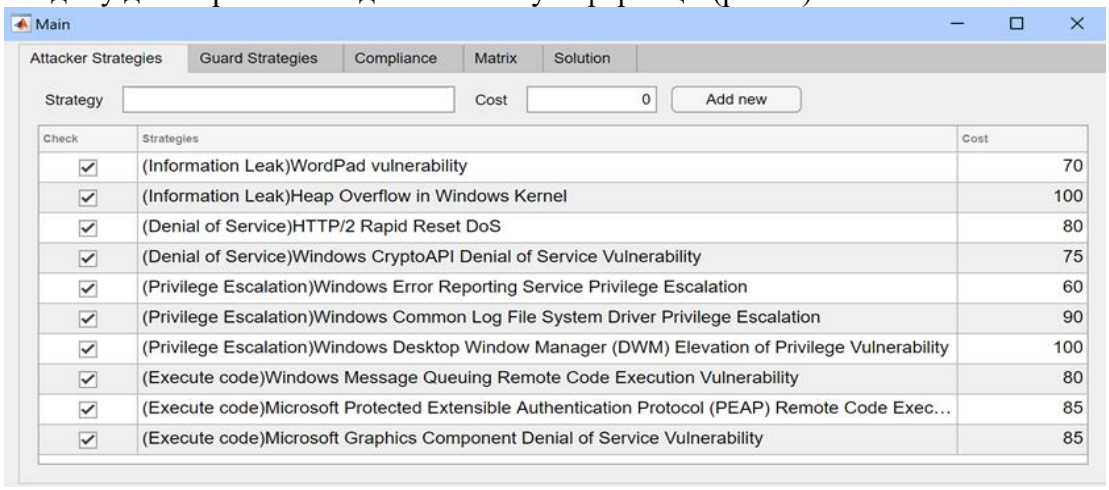


Рис. 1. Загальний вигляд головного вікна програмного застосунку

В окремих excel-файлах знаходяться списки стратегій зловмисника та адміністратора безпеки. При загрузці програми ці списки додаються у програму у відповідні таблиці на вкладках «Attacker Strategies» та «Guard Strategies». Вкладка «Compliance» відображає відповідність між стратегіями атакуючої та захищаючої сторони. Нулі в цій таблиці означають що відповідність стратегії атакуючої сторони та захищаючої не дає ніякого ефекту останнім. І навпаки, якщо в таблиці є одиниця значить даній стратегії атакуючого є протидіюча стратегія захищаючого.

Вкладка Matrix демонструє побудовану матрицю гри, згідно якої йде розрахунок гри. На вкладці «Solution» знаходиться рішення в заданій грі, а саме оптимальні чисті стратегії, якщо вони є та змішані стратегії, якщо вони потрібні (рис. 2).

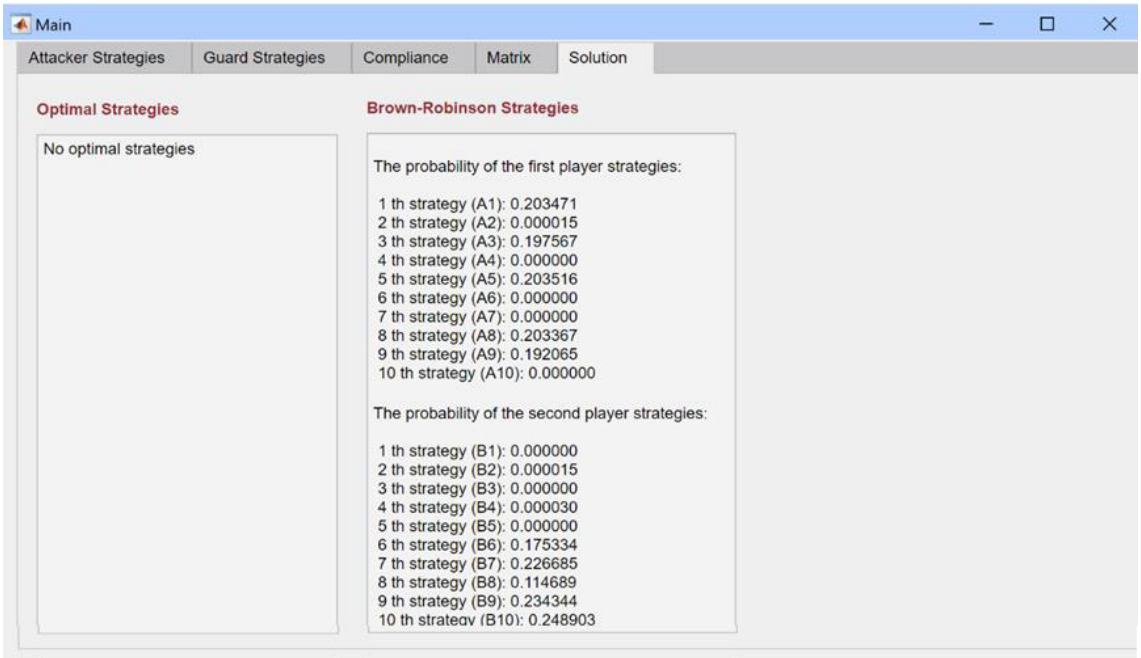


Рис. 2. Приклад рішення

Таким чином, в роботі запропонована методика рішення задач із захисту інформації. Методика використовує теорію ігор, а саме матричну гру двох гравців з нульовою сумою. Для пошуку оптимальних чистих стратегій використовується пошук сідлової точки. Для визначення змішаних стратегій використовується метод Брауна-Робінсона.

Список літератури

1. First. Загальна система оцінки вразливостей CVSS. URL: https://www.first.org/cvss/
2. Cvedetails. Поширені вразливості та ризики CVE. Вільний статистичний матеріал вразливостей стандарту CVE. URL: https://www.cvedetails.com/
3. Бартіш М. Я., Роман Л. Л. Теорія ігор. Львів: Видавничий центр ЛНУ, 2005. 120 с.

METHODS OF SOLVING PROBLEMS OF INFORMATION PROTECTION

V. Bilozerskyi, O. Lebedieva, N. Volkova, V. Nazarov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine;
e-mails: o.y.lebedieva@op.edu.ua, volkova.n.p@op.edu.ua, tasknavigator@gmail.com

The work developed a methodology for solving information protection problems. Cyber security is one of the most important problems of the modern world. The growing use of digital technologies in all areas of life makes cyberspace increasingly attractive to cybercriminals. Protection of information systems is one of the most important tasks of any security service of any organization and any enterprise. To counter this threat, it is necessary to develop effective information protection methods. The work considers such tools as an open standard for assessing the severity of computer system security vulnerabilities CVSS and a database of well-known information security vulnerabilities CVE. It makes sense to use these tools to create a list of effective modern attacks. In addition, it is still necessary to decide on the available tools for protecting the organization's computer systems. Cybersecurity relies on various mathematical tools, one of which is game theory. Game theory is one of the tools that can be used to improve cyber security. The work uses two-player matrix games. The players are an attacker who attacks the computer system of some organization and a representative of the organization responsible for ensuring information protection. Game theory allows you to present the task of computer system protection in a mathematical form, which allows you to use the established criteria for finding optimal protection strategies, following which the administrator is able to eliminate, or at least minimize, information damage caused by an attacker. Finding optimal pure strategies involves finding a saddle point. Not every matrix game has an optimal pure strategy. If the matrix game has a saddle point, then the game has a solution in pure strategies and the study of the game ends by finding this point and the corresponding pair of pure strategies of the players. Otherwise, mixed strategies are used. To search for mixed strategies, it is suggested to use the Brown-Robinson method.

Key words: protection of information systems, game theory, matrix game, Brown-Robinson method.

DOI 10.15276/imms.v13.no3-4.243
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 243-251

МЕТОДИКА ПРОГНОЗУВАННЯ РЕЗУЛЬТАТІВ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Б.В. Гаврилюк, В.В. Гулич, В.В. Зоріло

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: vikazorilo@gmail.com

Вивчення інформаційно-психологічної безпеки ставить низку питань, пов'язаних із забезпеченням безпеки людини та збереженням її здоров'я у зв'язку з різними видами інформаційних загроз: чинення цілеспрямованого інформаційного впливу на населення через засоби масової інформації, Інтернет, яке може привести до негативних соціально-політичних наслідків; неповна реалізація прав громадян у сфері отримання та обміну достовірної інформації; провокування соціальної, міжнаціональної, релігійної напруженості через діяльність окремих ЗМІ; маніпулювання масовою свідомістю з використанням інформаційно-психологічного впливу тощо. Прогнозування результатів інформаційно-психологічного впливу – важлива і актуальна проблема не тільки в масштабах окремого індивіда, а й для національної безпеки держави. Мета даної роботи – підвищення ефективності прогнозування інформаційно-психологічного впливу шляхом модифікації моделі інформаційно-психологічного впливу, заснованої на аналізі факторів впливу. У роботі проведено огляд наявних моделей для прогнозування результатів впливу, з яких було обрано модель для модифікації, щоб покращити результати прогнозування. Результатом роботи є методика, що враховує канали інформаційно-психологічного впливу, емоційну складову мемів та методи протидії, які може використовувати протиборча сторона, що дозволило створити теоретичну основу для проведення подальших практичних досліджень. Отримані результати можна використовувати для прогнозування інформаційно-психологічного впливу на соціум та/або обирати методи протидії цьому впливу для зменшення його наслідків.

Ключові слова: інформаційно-психологічний вплив, прогнозування впливу, емоційна складова мема, інформаційно-психологічна операція.

Вступ. Сучасне суспільство переживає надзвичайно інтенсивний період інформаційних трансформацій, що викликає значні зміни в сприйнятті, осмисленні та реакціях на інформацію з боку громадськості. Вплив масової інформації, інтернет-платформ, соціальних мереж, а також різноманітних каналів комунікації стає ключовим фактором, що формує не лише переконання, але й поведінку суспільства в цілому. Останні десятиліття показали, що інформаційна сфера стала не лише засобом передачі даних, а й потужним інструментом впливу на суспільство. Швидкий розвиток технологій зробив інформацію доступною для широкого кола людей, але одночасно викликав проблему, яка пов'язана з розповсюдженням недостовірної або спотвореної інформації.

Порушення інформаційно-психологічного простору засобами інформаційно-психологічного впливу може спричинити серйозні наслідки, такі як соціальні напруження, втручання у політичні процеси, розпалювання конфліктів та загроза національній безпеці.

Інформаційно-психологічний вплив (ІПВ) – це вплив на свідомість особи та/або населення з метою внесення змін у поведінку або світогляд. Контроль над свідомістю особи чи соціуму дозволяє впливати через них на технічні системи, наслідки чого можуть бути фатальними.

В умовах протиборства сторона, яка перша зможе «перепрограмувати» соціальну частину соціо-технічної системи для своєї вигоди, здобуде перемогу. Тому багато вчених займаються вивченням цього питання (О.З. Анісімович-Шевчук, А.В. Дудатьєв, О.П. Войтович, І.І. Ліпатов, Г.А. Дробаха, К.Ю. Гунбін, І.В. Воробйова, Я.В. Мацегора, І.І. Приходько, О.В. Тімченко, М.І. Товма, В.І. Пасічник, С.Л. Ліпатова та інші), а протиборчі сторони витрачають величезну кількість ресурсів для проведення успішного ІПВ або ж захисту від нього.

Цей напрямок дослідження надзвичайно важливий у зв'язку зі зростанням інформаційних конфліктів, поширенням фейків та дезінформації через медіа та онлайн-платформи. Розробка ефективних та точних методів передбачення можливих наслідків інформаційно-психологічного впливу є важливим завданням для забезпечення стабільності та безпеки суспільства, а також національної безпеки.

Метою роботи є підвищення ефективності прогнозування інформаційно-психологічного впливу шляхом модифікації моделі інформаційно-психологічного впливу, заснованої на аналізі факторів впливу.

Щоб досягти мети, потрібно вирішити наступні задачі.

1. Дослідити фактори впливу, які використовуються при проведенні інформаційно-психологічного впливу.
2. Дослідити сучасні методики та моделі прогнозування результатів інформаційно-психологічного впливу на предмет неврахованих факторів.
3. Обрати модель інформаційно-психологічного впливу для модифікації шляхом внесення неврахованих факторів
4. Провести теоретичні випробування модифікованої моделі.

Основна частина. Інформаційно-психологічний вплив є феноменом, що описує вплив інформації на психологічний стан та поведінку людей у суспільстві. Він визначається сукупністю методів, технологій та стратегій, спрямованих на формування певних думок, переконань, чи вчинків у масовій аудиторії.

Це поняття охоплює широкий спектр впливів, які здійснюються через інформаційні канали, такі як соціальні мережі, медіаплатформи, рекламні кампанії, політичні промови тощо. Основною метою інформаційно-психологічного впливу є формування переконань, маніпулювання уявленнями та зміна поведінкових шаблонів у суспільстві. В якості факторів впливу слід розглядати канали впливу, емоційну складову інформації (мема), та можливі методи протидії з протиборчої сторони.

Важливою характеристикою того чи іншого каналу впливу є ймовірність потрапляння під його дію. Даний показник розраховується індивідуально в залежності від характеристик соціуму та умов середовища перебування та функціонування соціуму. Наприклад, Дослідження Національної академії Національної гвардії України було проведене в 2015 році на соціумі у складі військових [1]. В цьому дослідженні описані канали впливу, характеристика інформації, що впливає, та методи протидії впливу. Нижче наведено частину проведеного дослідження каналів впливу, звідки можна визначити, з якою вірогідністю певний канал може вплинути на військового. У другій колонці таблиці 1 зазначено сумарну імовірність

Таблиця 1

Вплив джерел інформації на свідомість особи

Канал впливу	Ймовірність впливу у %
Родина	58,46
Друзі	58,46
Телебачення	53,84

продовження таблиці 1

Періодичний друк	32,31
Спілкування між особами	61,54

Також в цьому дослідженні було проведено експеримент для визначення значущості (емоційна складова) інформації (мема), яка буде впливати на особу.

Мем – це спеціальна підготовлена одиниця інформації, інструмент здійснення ІПВ. Емоційна складова мема – характеристика сприйняття (додатне значення від 0 до 1) або несприйняття (від'ємне значення від -1 до 0) мема. Цей показник впливає на ефективність проведення ІПВ.

Результати дослідження [1] вказують, що коефіцієнт емоційної складової для демотивуючої інформації сягає 0.41, в той час як для провокуючої інформації – 0.29, для дискредитуючої – 0.3.

Можемо бачити, що демотивуюча інформація має найбільший рівень емоційної складової, оскільки націлена на потреби та цінності особи, що потрапляє під вплив. Важливо зауважити, що відповідь на демотивацію зазвичай визначається тоном та способом подачі інформації, що може суттєво вплинути на можливості особистості. Цей підхід може призвести до значного зниження внутрішньої мотивації та осмислення, що зі свого боку може спричинити втрату професійного інтересу та розчарування. Негативна інформація, спрямована на провокацію, частіше викликає реакцію у вигляді оборонної позиції, викликає гнів та бажання відповісти відповідним чином. Мета такої провокації полягає в тому, щоб вразити або втягнути найменш стійкі особистості у конфлікт чи ситуацію, що спричинить конфлікт. Інформація, яка спрямована на дискредитацію гідності та честі соціуму чи окремих осіб, може експлуатувати оборонні механізми самосвідомості особистості.

Розглянуті методи протидії в цьому дослідженні можуть надати змогу для вдалого придушення інформаційно-психологічного впливу та розробляти певні рекомендації по боротьбі з впливом. У роботі [2] було проведено аналіз місця засобів масової інформації, як інструмента для ведення інформаційної війни. У роботі [3] розглянуто математичні моделі розповсюдження інформаційної загрози, а також моделі, що описують процес інформаційного протистояння. Робота [4] аналізує процес проходження інформації через умовні шари: поява або ж створення первинної інформації, її представлення в медіа та засобах інформування і формування відповідних коментарів. Розробка класифікації методів маніпулятивного впливу, а також розробка структурних та аналітичних моделей маніпулятивного впливу, що орієнтований на засоби масової інформації наводиться у роботі [5]. В роботі [6] наводиться типова модель ІПВ в соціумі, тобто коли люди взаємодіють з невеликими групами інших людей. Також у роботі [7] описано, як можна представити інформаційно-психологічний вплив за допомогою кортежу, який буде формувати цільову модель, що визначатиметься певними ознаками інформаційно-психологічно впливу: є змінна, яка визначає простір, на який спрямовано вплив, за оцінкою автору простір інформаційно-психологічного впливу може бути безкінечним, саме тому він розбивається на деякі параметри, а саме час впливу, тобто тривалість застосування певних методів впливу на окремий простір, мету впливу – локальна чи часткова мета, яка зазвичай при досягненні цієї мети агресія припиняється. Виходячи з вищевикладеного, автор зробив висновок, що завдяки цієї цільової моделі відбувається процес виявлення ІПВ, а завдяки функціональній – ідентифікація його виду.

Але жодна з цих робіт не використовує системні підходи для побудови загальної моделі інформаційно-психологічного впливу, яка б враховувала

початковий стан об'єктів, які в подальшому будуть зазнавати деструктивних впливів.

У роботі [8] автори описують реалізацію інформаційно-психологічного впливу через декілька каналів інформації, що розглядаються як зовнішній та внутрішній канали. Одна з представлених у [8] моделей описує кількість змін у соціальній частині соціотехнічної системи наступною формулою:

$$N = N_n + N_0(1 - (1 - k_1 p_в)(1 - k_2 p_з)) \quad (1)$$

де N_n – кількість агентів;

N_0 – кількість елементів соціуму, на яких спрямовано вплив;

k_1, k_2 – коефіцієнти емоційної складової інформації відповідно для зовнішнього та внутрішнього каналів;

$p_в$, $p_з$ – ймовірність потрапляння під вплив зовнішнього та внутрішнього каналу відповідно.

Дана модель була обрана для подальшої модифікації. Базова модель (1) задовольняє загальні потреби при плануванні програми інформаційно-психологічного впливу, але для повного уявлення варто враховувати фактори, що будуть зменшувати ефективність проведення впливу, тобто методи протидії зі сторони, на яку буде спрямовано вплив. Також дана модель використовує два канали впливу, зовнішній та внутрішній. Тоді виникає питання, як точно розрахувати можливості потрапляння під вплив цих каналів. Наприклад, канал зовнішнього впливу $Kan = \{Zmid, Tv, Int, Rm, Sp, Sz, Ld\}$ в [8] розглядався як єдине ціле, але це не завжди відповідає дійсності. В реальності вплив може здійснюватись з одного, декількох, або ж всіх можливих каналів. Тоді модифікована модель матиме вигляд:

$$N = N_n + N_0\big(1 - (1 - k_1 p_{в1})(1 - k_1 p_{в2}) \dots (1 - k_1 p_{вn})(1 - k_2 p_з)(1 - k_2 p_{з1}) \dots (1 - k_2 p_{зn})\big), \quad (2)$$

де $p_{в1,в2,\dots,вn}$ – ймовірності потрапляння під вплив внутрішніх каналів впливу;

$p_{з1,з2,\dots,зn}$ – відповідно ймовірності потрапляння під вплив зовнішніх каналів впливу, інші параметри залишаються незмінними.

Але, як зазначалось вище, дана модель не враховує методи протидії зі сторони, яка перебуває під інформаційно-психологічним впливом. Очевидно, що протидія інформаційно-психологічному впливу буде проводитися в таких же каналах, в якому проводиться сам вплив, тоді ймовірність потрапити під протидію буде дорівнювати можливості потрапляння під канал впливу. Протидія впливу – це також інформація, яка буде характеризуватися коефіцієнтом емоційної складової. Тому протидія буде прямо впливати, а саме зменшувати коефіцієнт емоційної складової інформації, яка використовується для впливу. Отже модель матиме вигляд:

$$N = N_n + N_0\big(1 - (1 - (k_1 - Y_в)p_{в1}) \dots (1 - (k_1 - Y_в)p_{вn})(1 - (k_2 - Y_з)p_{з1}) \dots (1 - (k_2 - Y_з)p_{зn})\big) \quad (3)$$

де N_n – кількість агентів;

N_0 – кількість елементів соціуму, на яких спрямовано вплив;

$Y_в$,$Y_з$ – емоційна складова протидії для зовнішнього та внутрішнього каналів впливу відповідно;

k_1, k_2 – коефіцієнти емоційної складової інформації відповідно для зовнішнього та внутрішнього каналів впливу;

$p_{в1,в2,\dots,вn}$ – ймовірність потрапляння під вплив внутрішніх каналів впливу;

$p_{з1,з2,\dots,зn}$ – ймовірність потрапляння під вплив зовнішніх каналів впливу;

Варто зазначити, що параметри $Y_в$ та $Y_з$ можуть враховувати не один метод протидії, а їх сукупність, тобто:

$$Y_{\text{в}} = \sum_{i=1}^{n} Y_{\text{в}_i} \quad (4)$$

$$Y_{\text{з}} = \sum_{i=1}^{n} Y_{\text{з}_i} \quad (5)$$

де $Y_{\text{в}_i}$ та $Y_{\text{з}_i}$ – всі можливі методи протидії, що використовуються.

Для отриманої моделі (3) для прогнозування результатів інформаційно-психологічного впливу та базової моделі (1) було розроблено додаток для підрахунку змін у соціальній частині соціотехнічної системи. Проведено експеримент з однаковими вхідними даними (кількість агентів та осіб, що піддаються впливу, канали впливу та коефіцієнти емоційної складової інформації), але з урахуванням протидії. Отримані результати демонструють, наскільки наявність протидії зменшує частку змін у соціальній частині соціотехнічної системи. На рис. 1 показано порівняльні діаграми для оригінальної (ліворуч) та модифікованої (праворуч) моделей ІПВ.

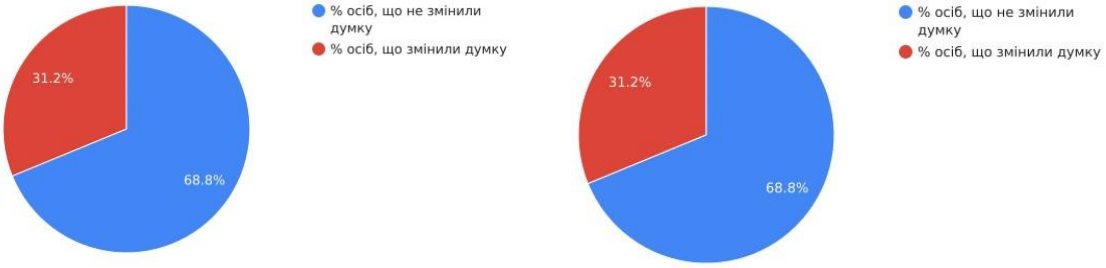


Рис. 1. Прогнозування результатів інформаційно-психологічного впливу

На рис. 2 наведені діаграми оригінальної моделі та модифікованої з розширеними (тобто обрано більше одного в кожному каналі) джерелами впливу (для внутрішнього каналу – колектив та наочні форми, для зовнішнього – релігійні організації, періодичний друк, телебачення). Для кожної моделі однакові вхідні дані: кількість агентів – 480, число осіб, на які спрямовано вплив – 21500, коефіцієнти емоційної складової інформації – 0,29 та 0,3 для внутрішніх та зовнішніх каналів відповідно.

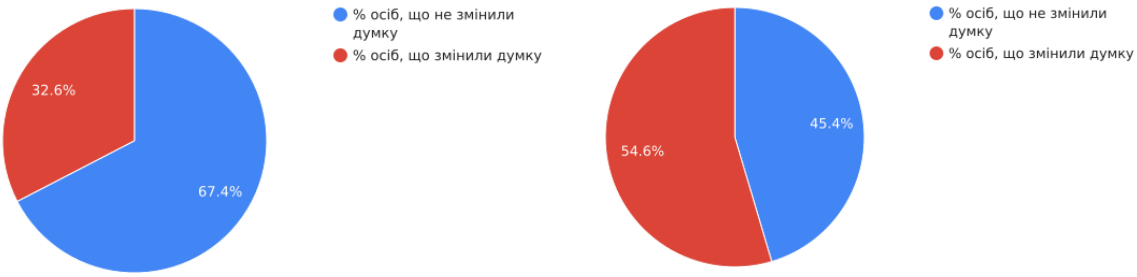


Рис. 2. Прогнозування результатів інформаційно-психологічного впливу

Таким чином, оскільки методи протидії обов’язково мають бути враховані, ми можемо бачити по отриманим результатам моделювання, що модифікована модель дійсно це відображає.

Оцінка емоційної складової мема – складний процес через суб’єктивність сприйняття інформації як окремою особою, так і соціумом. З врахуванням стрімкості розвитку технологій та, як наслідок, засобів і методів ІПВ, важливо мати можливість гнучко оцінювати цей показник мема. Як було зазначено, соціальні мережі – один із популярних Інтернет-сервісів для створення віртуальних спільнот, якими користується 90% користувачів українського Інтернету [9]. Їх використовують для комунікації, а також як засоби інформаційної боротьби (політичної, військової, релігійної і т.д.).

В Україні широкого поширення набув месенджер Telegram, який, як і соцмережі, також дозволяє створювати канали для масового поширення інформації.

Після початку повномасштабного вторгнення російської федерації 24 лютого 2022 року в Україні Telegram для багатьох людей став основним джерелом отримання інформації, а також дезінформації. За результатами дослідження, проведеного Київським міжнародним інститутом соціології у грудні 2022 року на замовлення Українського інституту медіа та комунікації (рис. 3), 63,3% українців почали читати телеграм-канали для отримання новин саме після 24 лютого 2022 року, тоді як до повномасштабного вторгнення таких було лише 35,9% [10].

Рис. 3. Графік результатів опитування серед респондентів

Поширення інформації в Telegram відбувається в основному через телеграм-канали. Телеграм-канали – це інструмент, який дозволяє користувачам створювати та управляти каналами, на які можуть підписуватися інші користувачі. Хоч в каналах лише адміністратор може публікувати повідомлення, але функції СМ передбачають зворотній зв'язок у вигляді реакцій, коментарів тощо.

Для дослідження будуть обрані телеграм-канали, в яких відсоток підписників, які читають пости за останні 30 днів (ERR_m), становить більше 10% від загальної кількості підписників. Це рішення прийнято, спираючись на дослідження вчених з американського Політехнічного інституту Ренсселера.

Дослідження виявило, щоб отримати механізм управління думкою певної соціальної групи, необхідно завербувати лише 10% від цієї групи. Тому при здійсненні ІПВ мемами через телеграм-канали необхідно впливати мінімум на 10% від усієї аудиторії телеграм каналу.

Для конкретики розглянемо телеграм-канал «Лачен пише», який має наступні характеристики (табл.2)

Таблиця 2

Характеристики каналу

Кількість підписників	Політична позиція каналу	Мова контенту	Тематика каналу	ERR_m
1 320 355	проукраїнський	українська	Політика	46,2%

Коефіцієнт емоційного складової мему позначимо *s*. Його також можна визначити як ймовірний відсоток того, що інформаційно-психологічний вплив викличе необхідну емоцію соціальної частини соціо-технічної системи (СТС), на яку здійснюється вплив. Тобто, якщо первина емоційна складова мему – це негативна емоція, то і викликати він повинен негативні емоції. Якщо при здійснені ІПВ викликається протилежна емоція від первинної, то можна вважати, що вплив буде не успішним, а коефіцієнт *s* – від'ємним.

В телеграм є можливість не просто ставити лайки/дизлайки, а реагувати за допомогою певного емодзі, який є підходящим для вираження ширшого спектра емоцій після взаємодії з мемом. Основним параметром оцінки буде енергія мема, яка може бути позитивною (E+) та негативною (E-).

Кожний емодзі, поставлений під мемом, буде розглядатися як одиниця енергії.

За одиницю позитивної енергії буде вважатися емодзі, який виражає емоцію, що співпадає з первинної емоційною складовою мема, через яку здійснюється інформаційно-психологічний вплив. Інакше емодзі будемо вважати одиницею негативної енергії.

За час впливу мему (час життя мему) буде обраний оптимальній період, коли основна більшість аудиторії його перегляне, а саме t = 24 год. Час дії впливу може бути збільшений, якщо на мем буде повторно звернено увагу додатковою інформацією або репостом в інший телеграм канал з вказаним першоджерелом.

Після того, як час життя мему сплине, підрахуємо енергію мему. Для демонстрації розглянемо мем з найбільшою кількістю негативної енергії (рис. 4).

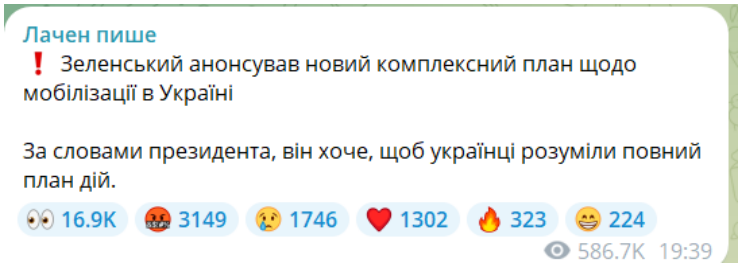


Рис. 4. Мем з найбільшою кількістю негативної енергії

Перед початком визначення емодзі з негативною/позитивною енергією треба провести аналіз мема:

- форма подання мему (Fpd): візуальна, однорідна у вигляді тільки тексту;
- інформаційний контент (Inf): однорідний, в мемі є тільки текст;
- складність структури: головна емоційно-забарвлена інформація, виділена великим червоним знаком оклику, доповнюється коментарем, який виконує функцію «згладжування вуглів»;
- мета ІПВ мему: зменшення негативних емоцій та привернення уваги до події.

Спираючись на попередній аналіз, класифікація емоцій для цього мему буде наступна:

- Емодзі з очима – характеризує, те що люди будуть спостерігати надалі за розвитком подій. Оскільки одна з цілей ІПВ – привернення уваги, то дану реакцію будемо відносити до позитивних.
- Емодзі з червоним смайлом – характеризує гнів, лайку в даному випадку, оскільки цей емодзі не відповідає меті ІПВ, негативна енергія;
- Емодзі з плачучим смайлом – означає жалість або смуток, не відповідає меті ІПВ, негативна енергія;
- Емодзі серця – означає згоду або вподобання, позитивна енергія;
- Емодзі вогню – характеризує підтримку, крутість, задовольняє меті інформаційно-психологічного впливу, позитивна енергія;
- Емоція усміхненого смайлу – зазвичай виражає радість або сміх, може символізувати сарказм, в даному випадку віднесемо до позитивної енергії.

Розібравшись з класифікацією емодзі відповідно до первинного змісту мему і мети ІПВ, можна визначити кількість певної енергії отриманої мемом. На основі отриманих даних можна спрогнозувати можливе значення коефіцієнта s. Розрахуємо його як відношення негативної енергії мему до загальної кількості

реакцій. Таким чином можна визначити рівень стійкості системи для певного мему з його первинним змістом і дослідити, як система реагує на певний мем [11]: система вважається стійкою, коли $0 \leq s \leq 0{,}4$, умовно стійкою, якщо $0{,}4 < s \leq 0{,}6$, нестійкою, якщо $0{,}6 < s \leq 1$.

В випадку, який був розглянутий, коефіцієнт $s = 0{,}2$. Це свідчить, що інформаційна система, яку представляє телеграм-канал «Лачен пише», стійка для даного мема.

Даний спосіб визначення коефіцієнта емоційної складової мема можна використовувати як один з параметрів в моделі (3).

Висновки. В роботі було досліджено і описано технології і способи, що використовуються для проведення інформаційно-психологічного впливу на суспільство. Модифіковано модель інформаційно-психологічного впливу. Отримана модель враховує методи протидії інформаційно-психологічному впливу та дозволяє прогнозувати інформаційно-психологічний вплив на соціум та обирати методи протидії цьому впливу для зменшення його наслідків.

Запропоновано метод визначення коефіцієнта емоційної складової конкретного мема, що дозволяє встановити ступінь стійкості соціо-технічної системи на прикладі конкретних телеграм-каналів.

Запропонована модифікація моделі та методика прогнозування інформаційно-психологічного впливу формують теоретичну основу для подальшого дослідження інформаційно-психологічних операцій в реальних умовах, що є предметом подальших досліджень.

Список літератури

1. Ліпатов І.І., Дробаха Г.А., Гунбін К.Ю. Протидія негативному інформаційно-психологічному впливу на особовий склад Національної гвардії України в умовах масових заворушень: монографія. Х.: Нац. акад. НГ України, 2015. 229с.URL:https://books.ndcnangu.co.ua/knigi/Monografija_protidija_vujs%27k_aspekt_nezakon2015.pdfhttps://www.researchgate.net/publication/312922994_The_ELK_Stack_in _Production
2. Хорошко В. О. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. *Інформаціційна безпека*. 2016. № 22 (3). С.283 – 288.
3. Tan C., Friggeri A., Adamic L. Lost in Propagation? Unfolding News Cycles from the Source. *Proceedings of the Tenth International Conference on Web and Social Media*, 2016. Vol. 10. No 1. P. 378-387. URL:http://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13011
4. Михайлов А. П., Маревцева Н. А. Модели информационной борьбы. *Математическое моделирование*. 2011. Т. 23. №10. С.19–32. URL: http://www.mathnet.ru/php/archive.phtml? wshow=paper&jrnid=mm&paperid=3162&option_lang=rus 05.12.2023
5. Gnatyuk S., Zhmurko T. Information-Psychological Security of Society in the Context of Information Warfare. Inżynier XXI wieku projectujemy przyszlosc, monografia. Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. S. 321 – 341.
6. Гріга В.С, Гізун А.І. Аналіз сучасних інформаційно-психологічних впливів в аспекті інформаційного протиборства. URL: https://core.ac.uk/download/pdf/84825492.pdf
7. Гріга В.С. Цільова та функціональна моделі інформаційно-психологічного впливу. URL: https://elartu.tntu.edu.ua/bitstream/lib/21650/4/X_VSNTK_2017v1_Hriha_VTsilova_ta _funktsionalna_modeli_49__COVER.jpg
8. Дудатьєв А. В., Войтович О.П. Інформаційна безпека соціотехнічних систем: модель інформаційного впливу. *Інформаційні технології та комп'ютерна інженерія*. 2017. Т.38. №1. С. 16-21.

9. Улічев О.С. Модель та методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства. URL: https://er.nau.edu.ua/bitstream/NAU/49742/1/dis_Ulichev.pdf
10. Як функціонують та завойовують аудиторію неінституціоналізовані новинні телеграм-канали українського сегменту. URL: https://www.jta.com.ua/wp-content/uploads/2023/02/Telegram-Channels-2023.pdf
11. Дудатьев А.В., Лужецкий В.А., Коротаев Д.А. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны. URL:https://media.neliti.com/media/publications/306626--a75eb896.pdf

METHODOLOGY FOR PREDICTING THE RESULTS OF INFORMATION AND PSYCHOLOGICAL INFLUENCE

B.V. Havryliuk, V.V. Hulych, V.V. Zorilo

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: vikazorilo@gmail.com

The study of information and psychological security raises a number of issues related to ensuring human security and preserving human health in connection with various types of information threats: targeted information influence on the population through the media, the Internet, which can lead to negative socio-political consequences; incomplete realisation of citizens' rights to receive and exchange reliable information; provoking social, ethnic, religious tensions through the activities of certain media; manipulation of Predicting the results of information and psychological influence is an important and urgent problem not only on the scale of an individual, but also for the national security of the state. The purpose of this paper is to increase the efficiency of forecasting information and psychological influence by modifying the model of information and psychological influence based on the analysis of influence factors. The paper reviews existing models for predicting the results of influence, from which a model was selected for modification to improve the forecasting results. The result of the work is a methodology that takes into account the channels of information and psychological influence, the emotional component of memes and the methods of counteraction that can be used by the opposing side, which allowed to create a theoretical basis for further practical research. The results obtained can be used to predict the information and psychological impact on society and/or to choose methods of counteracting this impact to reduce its consequences.

Keywords: information and psychological influence, forecasting of influence, emotional component of meme, information and psychological operation.

DOI 10.15276/imms.v13.no3-4.252
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 252-258

ЗАХИСТ ЛОКАЛЬНОЇ МЕРЕЖІ ВІД DDOS-АТАК НА ОСНОВІ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

М.Ю. Душейко, І.І. Бобок

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: men1ster69@gmail.com

Дослідження висвітлює важливість та актуальність атак SYN-flood в сучасному цифровому середовищі, з особливим акцентом на маршрутизатори як першу ланку оборони. DDoS-атаки, що використовують методологію SYN, продовжують представляти серйозну загрозу для стабільності та безпеки мережевих інфраструктур. Аналізуючи сучасний ландшафт кіберзагроз, висвітлюється масштабність та частота DDoS-атак SYN-flood, що ставлять під загрозу роботу маршрутизаторів. Зазначається, що еволюція таких атак включає в себе використання ботнетів, розподілені мережеві ресурси та інтелектуальні техніки, ускладнюючи виявлення та стримування. Основний фокус дослідження спрямований на роль маршрутизаторів як першої ланки оборони. З'ясовується, як SYN-flood впливають на працездатність мережевого обладнання, зокрема, на маршрутизатори, та аналізуються вимоги щодо ефективного захисту на цьому рівні. Дослідження розглядає сучасні технології та стратегії захисту, зокрема в контексті маршрутизаторів, які можуть виявити та мінімізувати вплив SYN-flood. Зацікавленість у використанні новітніх методів, таких як TCP SYN Cookies та інші технології, які ефективно контролюють аномальний трафік, є ключовою темою дослідження. Результати дослідження слугують як підстава для розробки та впровадження ефективних стратегій захисту на рівні маршрутизаторів, спрямованих на забезпечення стабільності та безпеки мережевих інфраструктур у зоні постійних DDoS-нападів SYN-flood.

Ключові слова: мережа, захист від DDoS, TCP SYN атака

Вступ. У сучасному цифровому ландшафті, де надійність та безпека мережевих інфраструктур є визначальними факторами для функціонування практично всіх аспектів суспільства та бізнесу, DDoS-атаки, зокрема ті, що використовують методологію SYN, залишаються актуальним та наростаючим викликом. SYN-flood, які використовують недоліки в рукостисканні протоколу TCP, визначаються своєю ефективністю та здатністю перевантажувати мережеве обладнання, ставлячи під загрозу нормальне функціонування мереж та серверів.

Сучасні зловмисники все частіше вдаються до вдосконалення та інтенсифікації DDoS-атак SYN-flood, використовуючи розподілені мережеві ресурси, техніку ботнетів та інтелектуальні алгоритми. Це призводить до збільшення масштабів та частоти атак, внаслідок чого виникає загроза для стійкості і доступності інтернет-служб, бізнес-процесів та загальної безпеки мережевого оточення.

Враховуючи важливість мережевих технологій у всіх сферах життя, вирішення проблем, пов'язаних з DDoS-атаками SYN-flood, стає критичною задачею. Аналіз та впровадження захисних стратегій на рівні маршрутизаторів, як ключової ланки оборони, визначаються необхідністю забезпечення стійкості мереж та збереження нормального функціонування в умовах надмірного трафіку та кіберзагроз.

Для вирішення цієї проблеми, важливо вдосконалювати технології та механізми захисту на рівні маршрутизаторів. Нові стратегії, такі як використання TCP SYN Cookies, які динамічно генерують ідентифікатори для нових підключень, або інші інтелектуальні методи фільтрації трафіку, стають важливими для забезпечення ефективного протистояння атакам SYN-flood.

Однак існує інша аспект актуальності, пов'язаний із здатністю атак SYN-flood еволюціонувати та адаптуватися до сучасних заходів захисту. Зловмисники використовують технології штучного інтелекту та машинного навчання для вдосконалення своїх стратегій та обхід заходів безпеки. Це ставить виклик перед розробниками та адміністраторами мережевих систем у пошуках найбільш інноваційних та ефективних заходів захисту.

Отже, забезпечення стійкості мереж і ефективності маршрутизаторів в умовах постійно зростаючих DDoS-атак SYN-flood є проблемою першочергового значення, вимагаючи постійного вдосконалення технік захисту та впровадження інноваційних підходів для забезпечення надійності і безпеки мережевих інфраструктур.

Мета статті та завдання дослідження. Метою цієї статті є розробка більш ефективного алгоритму для блокування DDoS атак, що використовують SYN пакети, на маршрутизаторі.

Для досягнення мети статті необхідно вирішити такі завдання:

1. Розібратися куди йдуть ресурси маршрутизатора під час використання технології TCP SYN COOKIES
2. Розробити більш ефективний алгоритм блокування користувачів

Основна частина. TCP SYN Cookies представляють собою ефективний механізм захисту від атак SYN-flood в контексті рукостискання протоколу TCP. Вони були розроблені для того, щоб забезпечити надійний та ефективний спосіб виявлення та захисту від DDoS-атак, зокрема тих, які використовують вразливості у початковому етапі встановлення TCP-з'єднань.

Основна ідея полягає в тому, щоб уникнути виділення ресурсів для зберігання стану непідтверджених з'єднань на сервері до того моменту, поки не буде отримано підтвердження від клієнта. Замість збереження повного стану підключення, сервер генерує унікальний ідентифікатор для кожного нового SYN-запиту, що надсилається клієнтом.

Коли клієнт повертається з підтвердженням (ACK), сервер може відновити повний стан підключення за допомогою збереженого ідентифікатора та інших відомостей, необхідних для правильної обробки. Якщо SYN-підтвердження не отримано протягом певного часового інтервалу або якщо відбувається яка-небудь аномалія, ідентифікатор видаляється, звільнюючи ресурси, і тим самим ускладнюючи здатність атакувати велику кількість непідтверджених з'єднань.

Переваги TCP SYN Cookies включають в себе ефективне використання обмежених ресурсів сервера, уникнення переповнення буферів та забезпечення надійного виявлення атак SYN-flood. Однак, слід враховувати, що використання TCP SYN Cookies може мати певне обчислювальне навантаження при генерації та обробці унікальних ідентифікаторів для кожного нового підключення.

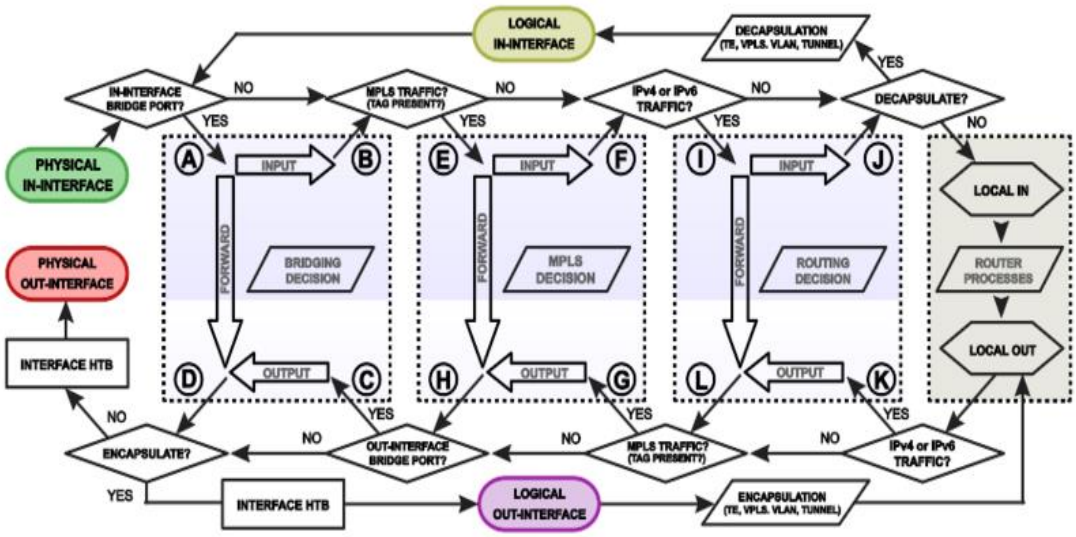


Рис. 1. Алгоритм обробки пакетів маршрутизатором [6]

Одним з недоліків TCP SYN Cookies, пов'язаних з обробкою пакетів SYN на маршрутизаторі під час DDoS-атаки, є повне проходження пакету через усі етапи обробки (рис. 1), включаючи внутрішні механізми, такі як розбір заголовків та перевірка правил фільтрації. Цей процес вимагає великої кількості ресурсів маршрутизатора і може призвести до суттєвого навантаження під час масштабних атак.

Під час SYN-flood, зловмисники штучно генерують великий потік SYN-запитів, намагаючись переповнити ресурси сервера. Коли кожен з цих запитів повинен повністю пройти всі етапи обробки на маршрутизаторі, це створює значне навантаження на процесор та пам'ять обладнання.

Такий підхід сприяє великій кількості витрачених ресурсів на обробку фальшивих або неправомірних SYN-запитів, витрачаючи пропускну здатність та обчислювальні ресурси на те, щоб визначити, чи ці пакети є легітимними.

У зв'язку з цим, розглядається проблема асиметричного навантаження на мережеве обладнання під час DDoS-атаки, коли великий обсяг SYN-запитів призводить до надмірного використання обчислювальних ресурсів маршрутизатора. Це може призвести до зниження продуктивності мережі, а в деяких випадках і до відмови обладнання під впливом атаки.

При вивченні ефективності методів захисту від шкідливого трафіку, виникає ключовий аспект щодо взаємозв'язку між захистом мережі та обробкою легітимного трафіку. Відключення інтерфейсу для блокування шкідливого трафіку, хоч і є ефективним заходом, водночас створює великі труднощі для нормальної обробки легітимних з'єднань.

У разі відключення інтерфейсу для блокування атаки, весь трафік, включаючи легітимний, також піддається призупиненню. Це може призвести до серйозних проблем з надійністю та доступністю мережі, оскільки легітимні користувачі чи служби не можуть взаємодіяти з мережею протягом цього часу.

З іншого боку, обробка шкідливого трафіку на рівні заголовків IP-пакетів надає можливість раннього виявлення та фільтрації потенційно небезпечних пакетів, не призупиняючи легітимний трафік. Це забезпечує нормальне функціонування легітимних з'єднань

При глибокому аналізі алгоритму обробки пакетів на рівні IPv4 та IPv6 в мережевих стеках маршрутизаторів, виявляється, що блокування з'єднань на етапі prerouting та в ланцюжку RAW PREROUTING може бути ефективнішим та оптимальним з точки зору забезпечення безпеки та продуктивності мережі.

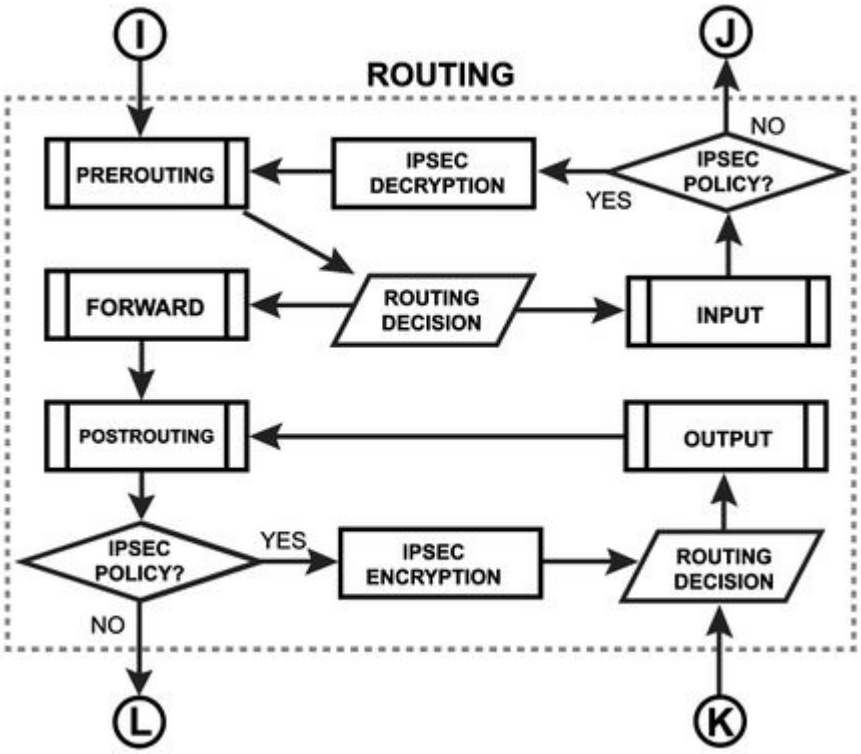


Рис. 2. Алгоритм обробки для IPv4 та IPv6 пакетів [6]

На етапі prerouting (рис. 2) пакети обробляються до того, як вони навіть дійдуть до основної обробки та будуть дешифровані. Це раннє втручання в обробку пакетів дозволяє вжити заходів безпеки до виконання всіх інших операцій, таких як маршрутизація.

Блокування на цьому етапі може значно зменшити навантаження на інші частини мережевого стеку, так як пакети, які не відповідають правилам безпеки, можуть бути відхилені ще до подальших етапів обробки.

Ланцюжок RAW PREROUTING (рис. 3) є частиною фільтрації пакетів на ранньому етапі, де вони ще не взяли участь в розборі TCP або інших високорівневих протоколів.

Блокування на цьому етапі дозволяє забезпечити максимальну ефективність, оскільки не виникає необхідності витрачати ресурси на повний розбір пакетів, якщо вже відомо, що вони мають бути відхилені.

Вищезазначені етапи є перспективними для застосування заходів безпеки, оскільки вони дозволяють максимально раннє виявлення та відхилення шкідливого трафіку, забезпечуючи тим самим збереження пропускної здатності та ефективність мережі. Блокування на етапі prerouting та ланцюжку RAW PREROUTING є ключовими компонентами комплексної стратегії безпеки мережі.

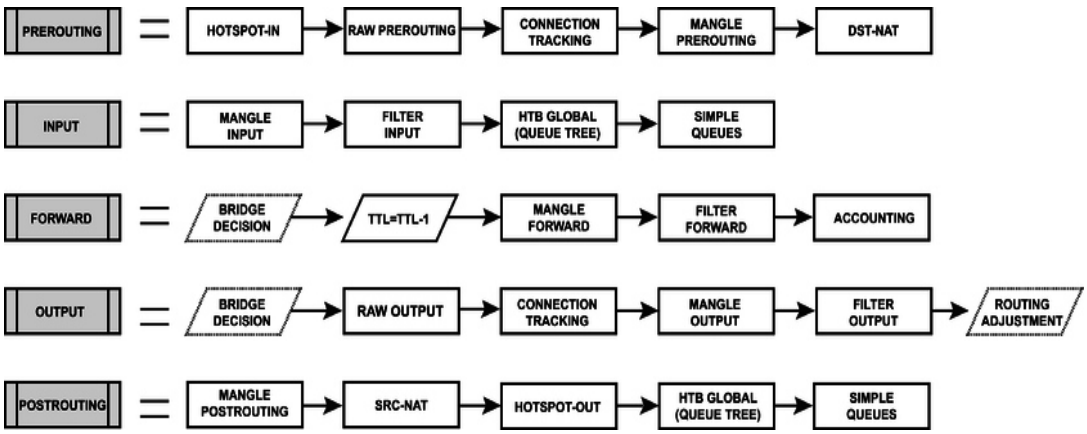


Рис. 3. Ланцюжки поетапної обробки IPv4 та IPv6 пакетів

Після визначення основних аспектів стратегії блокування шкідливого трафіку, наступним важливим кроком є визначення критерію, за яким буде відбуватися блокування. У вашому випадку, як тестовий критерій використовується кількість відправлених користувачем SYN-пакетів для встановлення сесій.

Кількість відправлених SYN-пакетів може служити важливим критерієм, оскільки SYN-flood часто характеризуються великою кількістю штучно згенерованих SYN-запитів, спрямованих на атаковану систему.

Критерій включає в себе порогове значення, яке визначає максимально припустиму кількість SYN-пакетів протягом певного часу. Якщо цей поріг перевищений, може ввімкнутися блокування для подальшого обмеження або відхилення трафіку від джерела атаки.

При досягненні порогового значення можуть застосовуватися заходи безпеки, такі як блокування IP-адреси або відхилення пакетів від цього джерела.

Використання критерію кількості відправлених SYN-пакетів є розумним і враховує специфіку атак SYN-flood flood. Адаптуючи його до конкретних умов та особливостей мережі, можна створити ефективний механізм блокування, який сприятиме захисту від потенційних атак та забезпечить стабільну роботу мережі.

Рис. 4. Алгоритм обробки пакетів маршрутизатором з блокуванням шкідливого трафіку

На основі всього вище згаданого можна розробити наступний алгоритм боротьби з атакою SYN-flood flood використовуючи ефективний підхід для виявлення та блокування потенційно шкідливого трафіку. Давайте розглянемо кожен крок цього алгоритму більш детально:

1. Програма, яка працює на самому маршрутизаторі, веде журнал сесій проходження трафіку через маршрутизатор. Це включає інформацію про кожну сесію, зокрема IP-адресу користувача та кількість відправлених SYN-пакетів.

2. Програма аналізує журнал сесій та визначає користувачів, кількість сесій яких перевищує порогове значення. Це може служити індикатором потенційної атаки SYN flood.

3. Після виявлення перевищення порогу, програма передає IP-адресу відповідного користувача до маршрутизатора для подальших заходів блокування.

4. Маршрутизатор обробляє отриману IP-адресу у ланцюжку RAW PREROUTING. Це дозволяє вжити заходів безпеки на ранньому етапі обробки пакетів, перед тим як вони будуть повністю розгортатися вищими рівнями стеку.

5. Маршрутизатор блокує вказану IP-адресу, запобігаючи прийняттю подальших SYN-пакетів від цього джерела. Це ефективно обмежує можливість здійснення нових сесій від атакуючого користувача.

6. Після блокування IP-адреси програма видаляє всі сесії цього користувача з журналу сесій маршрутизатора. Це сприяє оптимізації використання ресурсів маршрутизатора та збереженню пропускної здатності.

Запропонований алгоритм дозволяє вчасно реагувати на підозрілі активності, блокувати потенційно шкідливий трафік та захищати ресурси маршрутизатора від надмірного навантаження під час атак SYN flood.

Висновки. У статті розглянуто питання захисту від атак SYN-flood на маршрутизаторах. Пройшли через основні проблеми, що виникають при таких атаках, і висвітлили ключові стратегії та технології для їх ефективного управління.

Розглянули актуальність DDoS атак SYN-flood сьогодні, зазначивши їхню загрозливість для нормального функціонування мереж та сервісів. Детально розглянули механізм захисту від SYN атак на маршрутизаторах, зокрема, зробили акцент на використанні технології TCP SYN COOKIES, яка спрямована на зменшення навантаження на процесори обладнання.

Відзначили, що відсічення шкідливого трафіку на етапі обробки заголовків IP-пакетів є доцільнішим, оскільки це дозволяє забезпечити ефективний захист мережі без втрати пропускної здатності та надійності.

Також розглянули ефективний підхід до боротьби з SYN-flood, який включає в себе ведення детального журналу сесій, виявлення порушень, передачу інформації до маршрутизатора, блокування айпі адрес та оптимізацію використання ресурсів.

За статтю розкрито важливі аспекти та стратегії в області захисту від атак SYN-flood flood, зокрема на маршрутизаторах, що сприяє покращенню безпеки та стійкості мереж проти цих загроз.

Усе вищезазначене свідчить про важливість та актуальність розробки та впровадження ефективних заходів безпеки для захисту мережевого обладнання від атак DDoS, зокрема, від атак SYN-flood. Відділення шкідливого трафіку на ранньому етапі обробки пакетів, використання інтелектуальних алгоритмів та технік, є необхідними компонентами сучасних стратегій кібербезпеки.

Запропоновані методи аналізу та реакції на аномалії у вигляді блокування IP-адрес при досягненні порогових значень сесій дозволяють виявляти та ефективно обмежувати шкідливий трафік, забезпечуючи при цьому збереження ресурсів та продуктивності мережі.

В цілому, захист від атак SYN-flood на маршрутизаторах вимагає інтегрованого та ретельно продуманого підходу, оскільки ці атаки можуть суттєво підірвати працездатність мережі та послуг. Розробка та вдосконалення таких заходів безпеки є важливим елементом у забезпеченні стабільності та надійності сучасних мережевих інфраструктур.

Список літератури

1. RFC 4987. TCP SYN Flooding Attacks and Common Mitigations. 2007. P. 6-10
2. RFC 6013. TCP Cookie Transactions (TCPCT). 2011. P. 4-25
3. DARPA. Internet Program Protocol Specification. Information Sciences Institute. University of Southern California,1981, P. 15-52
4. RFC 9293. Transmission Control Protocol (TCP). 2022
5. Gont F. SI6 Networks. Defending against Sequence Number Attacks . UTN-FRH S. Bellovin Columbia University, 2012
6. MikroTik Packet Flow v6. URL: https://blog.telecom-sales.ru/mikrotik-packet-flow-v6-shemy-prohozhdeniya-trafika/

LOCAL NETWORK PROTECTION AGAINST DDOS ATTACKS BASED ON NETWORK TRAFFIC DATA

M.Yu. Dusheyko, I.I. Bobok

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: men1ster69@gmail.com

The study highlights the importance and relevance of SYN attacks in today's digital environment, with a particular focus on routers as the first line of defense. DDoS attacks using the SYN methodology continue to pose a serious threat to the stability and security of network infrastructures. Analyzing the current landscape of cyber threats, the article highlights the scale and frequency of SYN DDoS attacks that jeopardize the operation of routers. It is noted that the evolution of such attacks includes the use of botnets, distributed network resources, and intelligent techniques, making them difficult to detect and deter. The main focus of the study is on the role of routers as the first line of defense. The study examines how SYN-type DDoS attacks affect the performance of network equipment, including routers, and analyzes the requirements for effective protection at this level. The study examines current technologies and defense strategies, particularly in the context of routers, that can detect and minimize the impact of SYN DDoS attacks. The interest in using the latest techniques, such as TCP SYN Cookies and other technologies that effectively control anomalous traffic, is a key topic of the study. The results of the study serve as a basis for the development and implementation of effective protection strategies at the router level aimed at ensuring the stability and security of network infrastructures in the area of constant SYN-type DDoS attacks.

Keywords: network, DDoS protection, TCP SYN attack.

DOI 10.15276/imms.v13.no3-4.259
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 259-265

МОДИФІКАЦІЯ АЛГОРИТМУ ВИЯВЛЕННЯ КЛОНУВАННЯ КАДРІВ У ВІДЕОПОСЛІДОВНОСТЯХ

О.В. Іларіонова, О.Ю. Лебедєва

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mails: o.y.lebedieva@op.edu.ua ilarionova.olga.l@gmail.com

В роботі розроблено модифікацію алгоритму виявлення клонування кадрів у відеопослідовностях. Життя сучасної людини неможливо уявити без постійної присутності у ньому цифрових технологій. Вони стали невід'ємною частиною нашого побуту. У кожного є смартфон, майже кожен володіє персональним комп'ютером або ноутбуком. Технології фото- та відеозйомки, а також розповсюдження та оприлюднення знімків і відео, такі, як соцмережі, зробилися невід'ємною частиною цифровізації. Цифровізація поширилась і на дуже важливі для життя людства сфери, такі от як криміналістика або засоби масової інформації. Для того, щоб мати довіру до відеоматеріалів, яка надзвичайно важлива у кримінальних розслідуваннях, судових справах та інформаційних мережах, потрібно розвивати сферу викриття модифікацій та фальсифікацій у відео- та фотоматеріалах, розробляти нові методи, що дозволяють впевнитися в цілісності відео або виявити фальсифікацію, та модифікувати і вдосконалювати вже розроблені. В роботі виконано аналіз методів для знаходження фальсифікацій у відеопослідовностях та сучасних форматів і алгоритмів для збереження і стискання відеопослідовностей. У результаті аналізу було виявлено поточний стан розвитку сфери виявлення підробок відео та визначено найпопулярніші відеоформати. Було проведено експерименти з відео різних форматів та роздільних здатностей, зібрано та проаналізовано дані, після чого встановлені необхідні порогові значення коефіцієнта кореляції Пірсона для кожного досліджуваного формату. В роботі було запропоновано порогові значення для пошуку клонованих кадрів. Порогове значення обирається в залежності від формату та роздільної здатності відео. Для модифікації алгоритму виявлення клонування кадрів у відеопослідовності шляхом аналізу порогових значень коефіцієнту кореляції Пірсона бралися такі параметри, як формат відео та роздільна здатність. Була створена програмна реалізація модифікації алгоритму виявлення клонування кадрів у відеопослідовностях. В роботі наводяться помилки першого та другого роду.

Ключові слова: цифрове відео, клонування кадрів, коефіцієнт кореляції, виявлення клонування кадрів.

Вступ. Життя сучасної людини неможливо уявити без постійної присутності у ньому цифрових технологій. Вони стали невід'ємною частиною нашого побуту. Технології фото- та відеозйомки, а також розповсюдження та оприлюднення знімків і відео, такі, як соцмережі, зробилися невід'ємною частиною цифровізації. Сучасна людина стикається з відео та фото всюди: гортає стрічку в Tik-Tok або Instagram у вільний від роботи час, дивиться рекламу або вірусні ролики, має у своєму телефоні безліч варіантів фото- та відеоспогадів про себе, членів сім'ї та своїх домашніх тварин.

Техніка та програми, що можуть обробляти фото та відео, також останнім часом зазнали великого розвитку. Для того, щоб ними користуватися, не потрібна спеціальна освіта, достатньо мати мінімальне обладнання та доступ в Інтернет.

Не тільки звичайні користувачі, а й злочинці тепер мають широкий інструменти для модифікації та фальсифікації фото та відео, що ускладнює задачу визначення правдивої інформації у купі інформаційного шуму. Багато людей

звикли гортати стрічку, швидко сприймати короткі відео, і не перевіряти інформацію прискіпливо. Отже, для обману тепер треба тільки щоб трохи пощастило, і відео побачила необхідна кількість людей. За допомогою такого прийому можна поширити фейк, згубити репутацію громадського чи політичного діяча тощо.

Отже, для того, щоб мати довіру до відеоматеріалів, яка надзвичайно важлива у кримінальних розслідуваннях, судових справах та інформаційних мережах, потрібно розвивати сферу викриття модифікацій та фальсифікацій у відео- та фотоматеріалах, розробляти нові методи, що дозволяють впевнитися в цілісності відео або виявити фальсифікацію, та модифікувати і вдосконалювати вже розроблені, тому робота є актуальною.

Мета та задачі роботи. Метою даної роботи є підвищення ефективності алгоритму виявлення клонування кадрів у відеопослідовностях шляхом модифікації за допомогою аналізу порогових значень.

В процесі досягнення мети виконуються наступні задачі:

- аналіз відеопослідовностей для отримання порогових значень для коефіцієнта кореляції;
- розробити модифікацію алгоритму виявлення фальсифікації у відеопослідовності;
- програмно реалізувати розроблену модифікацію алгоритму виявлення клонування кадрів у відеопослідовностях;
- оцінити ефективність розробленої модифікації алгоритму виявлення клонування кадрів у відеопослідовностях.

Під порушенням цілісності (фальсифікацією) цифрового відео у роботі розуміється застосування до відеопослідовності клонування кадрів, що проводиться засобами графічних редакторів відеопослідовностей.

Ефективність виявлення клонування кадрів оцінюємо кількістю помилок першого і другого роду.

Основна частина. Виявлення фальсифікації відео – це підкатегорія відеокриміналістики, яка досліджує відео щодо змін контенту і може визначити просторові або часові місця підробки. Підходи виявлення фальсифікації відео можуть бути як активними, так і пасивними в залежності від наявності апріорної інформації про відео.

Активні методи, такі як цифровий підпис та водяні знаки, вимагають попередньо вбудованої інформації досліджуваного файлу для перевірки його легітимності. Більшість пристроїв відеозахоплення, які представлені на ринку, не підтримують цю функцію. Крім того, це залежить від розсуду користувача, вбудовувати цю інформацію чи ні.

Пасивні чи приховані методи виявлення несанкціонованого доступу до відео не вимагають попередньої інформації для класифікації відео як підробленого чи ні. Ці методи є більш надійними у реальних сценаріях, оскільки вони працюють, використовуючи сліди або артефакти несанкціонованого доступу. В нашій роботі ми будемо використовувати саме пасивні методи виявлення фальсифікації відео.

Відео можна розглядати як послідовність зображень, які називаються кадрами, що відображаються протягом певного періоду часу. Таким чином, методи виявлення несанкціонованого доступу можуть застосовуватись лише на рівні кадру.

Під атакою на відеопослідовність будемо розуміти порушення цілісності цього відео. Порушення цілісності або фальсифікацію відео можна розділити на 3 категорії [1]:

- атаки просторового втручання, тобто внутрішньокадрові;
- атаки часового втручання, тобто міжкадрові;

– атаки просторово-часового втручання.

Фальсифікації можуть відбуватися на рівнях кадру, блоку, пікселю або сцени [2].

При внутрішньокадровій атаці змінюється вихідний вміст певних кадрів. Є декілька видів популярних операцій при внутрішньокадровій атаці:

– додавання певних областей та об’єктів з цього відео у кадрі;
– додавання певних областей та об’єктів з різних відео у кадрі;
– видалення деякого об’єкту з кадру;
– спотворення зображення за допомогою використання геометричних перетворень.

Атаки часового втручання, тобто міжкадрові підробки, відрізняються тим, що кадр піддається процесу фальсифікації повністю, а не частково. Можна виділити декілька типів міжкадрових фальсифікацій:

– видалення кадру з відео;
– вставку кадрів з інших відео;
– дублювання кадрів з поточного відео;
– перетасовку кадрів.

Видалення кадрів пов'язане з видаленням подій у відео шляхом видалення відповідних кадрів. При вставці кадрів кадри, скопійовані з одного відео, вставляються до іншого. Дублювання кадрів (або реплікація) включає копіювання кадрів у відео і вставку їх в інші тимчасові місця того ж відео. Перетасовування кадрів – це ще одна форма дублювання кадрів, коли скопійовані кадри переупорядковуються в часі перед вставкою. Вставка кадрів, дублювання кадрів та перетасовування кадрів можуть бути використані для заповнення пробілу у видалених кадрах у відео. В нашій роботі працюємо з дублюванням кадрів того ж відео.

Наразі цифрове відео, відзняте на сучасну камеру, само по собі багато важить. Для того, щоб оптимізувати розподіл доступного простору для збереження інформації і зменшити розмір відео, використовуються відеокодеки, які реалізовують конкретні алгоритми стиснення для відео. Двома ключовими методами стиснення, які використовуються, є дискретне косинусне перетворення (DCT) та алгоритм компенсації руху (Motion Compensation).

Стиснення буває внутрішньокадрове та міжкадрове. Внутрішньокадрове кодування – це техніка стиснення даних, яка використовується у відеокадрі, що дозволяє зменшити розміри файлів і знизити бітрейт із незначною втратою якості або без неї. Внутрішньокадрове прогнозування використовує просторову надмірність, тобто кореляцію між пікселями в одному кадрі, шляхом обчислення прогнозованих значень за допомогою екстраполяції з уже закодованих пікселів. При міжкадровому кодуванні розмір відеофайлу зменшується за рахунок кодування лише відмінностей між двома послідовними кадрами замість стиснення кожного кадру, тобто зберігаються лише зміни між двома послідовними кадрами, що призводить до значно менших розмірів файлів. Сучасні та найпоширеніші формати збереження відеопослідовностей це: AVI, MKV, MPEG-4, WMV, WebM. В роботі були використані 5 форматів відеофайлів: AVI, MKV, MP4, WebM та WMV. Для пошуку дубльованих кадрів у відеопослідовностях можуть бути використовувати метрики відстані. В якості метрики відстані в роботі використовується коефіцієнт кореляції Пірсона.

Коефіцієнт кореляції Пірсона використовується для виявлення взаємозв'язку між двома змінними, визначає, чи пропорційна їх мінливість, коли при зміні одного показника змінюється і другий. Кореляція Пірсона є лінійною. У математичній статистиці значення коефіцієнта кореляції Пірсона може бути від +1 до -1, де +1 свідчить про наявність повного позитивного лінійного зв'язку, а -1 —

про наявність повного негативного лінійного зв'язку. Для двох однакових зображень значення коефіцієнта кореляції Пірсона дорівнює 1.

Було проведено ряд експериментів, в яких відзняті оригінальні відео, кожне з яких розбивалось на кадри та виконувалось дублювання одного з кадрів на інше місце у відео. Фальсифіковане таким чином відео зберігалось в форматах зі втратами avi, mkv, mp4, WebM та wmv. Використовувалось відео з різною роздільною здатністю.

В попередній роботі було розроблено алгоритм виявлення клонування кадрів у відеопослідовностях, який ефективно працював з відеопослідовностями, які були збережені в форматах без втрат після фальсифікації. В даній роботі використовувалися відео збережені в форматах зі втратами, тому основним завданням експериментів було знайти порогові значення для коефіцієнта кореляції Пірсона для визначення дубльованих кадрів. Для цього у кожному відео знаходились значення коефіцієнта кореляції Пірсона між всіма кадрами відео. З даних було сформовано таблиці, де номера строк та рядків відповідають номерам кадрів у відео, а жовтим кольором замальовані значення коефіцієнта кореляції відповідні кадрам, які були клоновані. Для кожного формату та кожної роздільної здатності було зроблено окрему таблицю. В таблицях були проаналізовані значення коефіцієнту кореляції для дубльованих кадрів.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	0,00000	0,99972	0,99927	0,99833	0,99769	0,99578	0,99462	0,99456	0,99276	0,99276	0,99277	0,99277	0,99341	0,99284	0,99285	0,99281	0,99232	0,99232	0,99232	0,99232	0,99232
2	0,99972	0,00000	0,99943	0,99850	0,99784	0,99594	0,99474	0,99468	0,99288	0,99288	0,99288	0,99289	0,99346	0,99292	0,99292	0,99288	0,99241	0,99241	0,99241	0,99241	0,99241
3	0,99927	0,99943	0,00000	0,99901	0,99838	0,99645	0,99526	0,99520	0,99335	0,99335	0,99336	0,99336	0,99386	0,99333	0,99334	0,99329	0,99283	0,99283	0,99283	0,99284	0,99284
4	0,99833	0,99850	0,99901	0,00000	0,99934	0,99744	0,99625	0,99619	0,99433	0,99433	0,99433	0,99434	0,99461	0,99408	0,99409	0,99405	0,99361	0,99361	0,99361	0,99361	0,99361
5	0,99769	0,99784	0,99838	0,99934	0,00000	0,99800	0,99684	0,99678	0,99491	0,99491	0,99491	0,99492	0,99506	0,99453	0,99455	0,99450	0,99407	0,99408	0,99408	0,99408	0,99408
6	0,99578	0,99594	0,99645	0,99744	0,99800	0,00000	0,99871	0,99865	0,99671	0,99672	0,99672	0,99672	0,99618	0,99565	0,99566	0,99563	0,99521	0,99521	0,99521	0,99521	0,99521
7	0,99462	0,99474	0,99526	0,99625	0,99684	0,99871	0,00000	0,99990	0,99791	0,99791	0,99791	0,99791	0,99739	0,99687	0,99688	0,99684	0,99642	0,99643	0,99643	0,99643	0,99643
8	0,99456	0,99468	0,99520	0,99619	0,99678	0,99865	0,99990	0,00000	0,99799	0,99799	0,99799	0,99799	0,99746	0,99695	0,99695	0,99692	0,99650	0,99650	0,99650	0,99650	0,99650
9	0,99276	0,99288	0,99335	0,99433	0,99491	0,99671	0,99791	0,99799	0,00000	0,99999	0,99998	0,99998	0,99836	0,99862	0,99863	0,99862	0,99836	0,99836	0,99836	0,99836	0,99836
10	0,99276	0,99288	0,99335	0,99433	0,99491	0,99672	0,99791	0,99799	0,99999	0,00000	0,99998	0,99999	0,99836	0,99863	0,99863	0,99862	0,99836	0,99836	0,99836	0,99836	0,99836
11	0,99277	0,99288	0,99336	0,99433	0,99491	0,99672	0,99791	0,99799	0,99998	0,99998	0,00000	0,99999	0,99836	0,99862	0,99863	0,99862	0,99836	0,99836	0,99836	0,99836	0,99836
12	0,99277	0,99289	0,99336	0,99434	0,99492	0,99672	0,99791	0,99799	0,99998	0,99999	0,99999	0,00000	0,99836	0,99863	0,99863	0,99862	0,99836	0,99836	0,99836	0,99836	0,99836
13	0,99341	0,99346	0,99386	0,99461	0,99506	0,99618	0,99739	0,99746	0,99836	0,99836	0,99836	0,99836	0,00000	0,99932	0,99931	0,99926	0,99872	0,99872	0,99871	0,99872	0,99872
14	0,99284	0,99292	0,99333	0,99408	0,99453	0,99565	0,99687	0,99695	0,99862	0,99863	0,99862	0,99863	0,99932	0,00000	0,99997	0,99991	0,99932	0,99932	0,99932	0,99932	0,99932
15	0,99285	0,99292	0,99334	0,99409	0,99455	0,99566	0,99688	0,99695	0,99863	0,99863	0,99863	0,99863	0,99931	0,99997	0,00000	0,99992	0,99933	0,99933	0,99933	0,99933	0,99933
16	0,99281	0,99288	0,99329	0,99405	0,99450	0,99563	0,99684	0,99692	0,99862	0,99862	0,99862	0,99862	0,99926	0,99991	0,99992	0,00000	0,99939	0,99939	0,99939	0,99939	0,99939

Рис. 1. Приклад значень коефіцієнту кореляції у відеопослідовності

В таблиці 1 представлено знайдені порогові значення коефіцієнту кореляції Пірсона для кожного формату.

Таблиця 1

Порогові значення для коефіцієнту кореляції Пірсона

Формат відео	Роздільна здатність відео	Порогове значення
AVI	640x360	0,99995
	856x480	0,99993
	720x1280	0,99994
MKV	640x360	0,99998
	856x480	0,99997
	720x1280	0,99995
MP4	640x360	0,99998
	856x480	0,99997
	720x1280	0,99997
WebM	640x360	0,99995
	856x480	0,99995
	720x1280	0,99992
WMV	640x360	0,99999
	856x480	0,99998
	720x1280	0,99993

Будемо вважати, що маємо відеопослідовність з кадрів $P = \{p_1, p_2, \ldots, p_s\}$ розміру M x N, де s – кількість кадрів. Кожний кадр зберігається в форматі RGB. Для роботи алгоритму необхідно перетворити RGB в YUV і використовувати в обчисленнях тільки матрицю Y. Модифікований алгоритм виявлення клонування кадрів у відеопослідовності складається з наступних основних кроків:

Крок 1. Зчитується відео V, формат відео F та його роздільна здатність R.

Крок 2. Зчитується послідовність кадрів $P = \{p_1, p_2, \ldots, p_s\}$ із відео V розміру M x N.

Крок 3. Зчитується p_i кадр, i = 1, …, s. Маємо матрицю Y^i. Для кожного кадру p_i виконуємо наступні кроки:

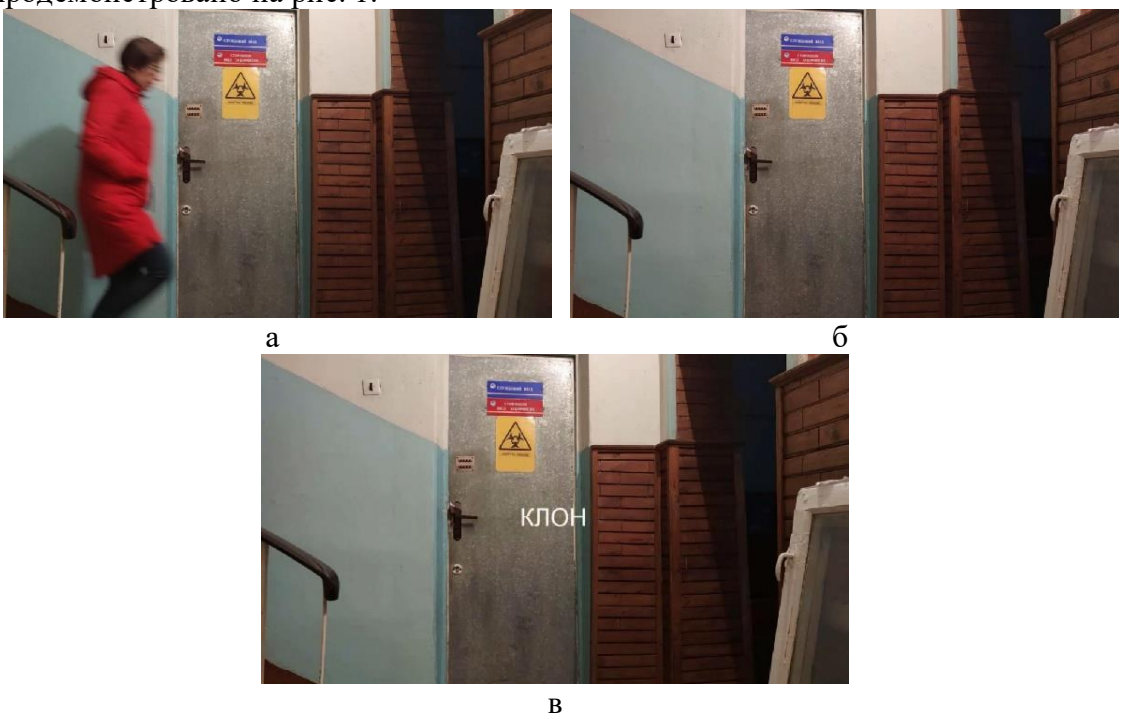
Крок 3.1 Зчитується p_j кадр, j = 1, …, s., $i \neq j$. Отримуємо матрицю Y^j. Для кожної пари кадрів p_i та p_j для матриць Y^i та Y^j вирахувати метрику подібності блоків коефіцієнт кореляції Пірсона $metric_{ij}$.

Крок 3.2. В залежності від F та R встановлюється порогове значення δ_{FR}.

Крок 3.3 Якщо $metric_{ij} \geq \delta_{FR}$, то кадри p_i та p_j є оригінальним та клонованим, запам’ятовуються їх номера, res = res U i U j. Інакше розглянути наступну пару кадрів.

Крок 4. Вивести знайдені номери кадрів res. Зберегти відео, що перевірялось з поміченим надписом «КЛОН» в дубльованих кадрах.

Розроблено програмний додаток, який реалізує модифікацію алгоритму виявлення клонування кадрів у відеопослідовності. Результати роботи програми продемонстровано на рис. 1.



а б

в

Рис. 2. Результати роботи модифікації алгоритму виявлення клонування кадрів у відеопослідовності: 36 кадр оригінального відео (а); 36 кадр фальсифікованого відео (б); результат роботи програми для 36 кадру (в)

При дослідженні помилкою першого роду будемо вважати клоновані кадри, які не було знайдено. Помилкою другого роду будемо вважати оригінальні кадри, які були розпізнані як клоновані. В таблиці 2 продемонстровано помилки першого та другого роду для кожного формату.

Таблиця 2

Помилки першого та другого роду

Формат	Роздільна здатність	Помилки першого роду, %	Помилки другого роду,%
AVI	640x360	4,33	7,03
	856x480	3,09	6,03
	720x1280	3,77	2,76
MKV	640x360	1,71	7,36
	856x480	1,96	4,69
	720x1280	0,99	2,26
MP4	640x360	1,97	7,36
	856x480	1,18	4,69
	720x1280	2,36	0,92
WebM	640x360	1,31	1,92
	856x480	3,54	0,84
	720x1280	2,36	2,59
WMV	640x360	1,71	1,09
	856x480	2,23	2,01
	720x1280	0,52	4,27

Таким чином, розроблена модифікація алгоритму виявлення клонування кадрів у відеопослідовності працює добре з визначеними пороговими значеннями при різних роздільних здатностях, у відео з різним видом освітлення та з рухомим чи нерухомим тлом.

Список літератури

1. Patel J., Sheth R. Passive video forgery detection techniques to detect copy move tampering through feature comparison and RANSAC. *Cyber security and digital forensics*. Singapore: Springer, 2022. P.161–177.
2. Amjed A., Mahmood B., Almukhtar K.A. Approaches for forgery detection of documents in digital forensics: A review. *International conference on emerging technology trends in internet of things and computing.* Cham: Springer, 2022. P. 335–351.
3. Sitara K., Mehtre B.M. Detection of inter-frame forgeries in digital videos. *Forensic Science International.* 2018. V.289. P. 186-206.

MODIFICATION OF THE ALGORITHM FOR DETECTION OF FRAME CLONING IN VIDEO SEQUENCES

O. Ilarionova, O. Lebedieva

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
e-mails: o.y.lebedieva@op.edu.ua ilarionova.olga.l@gmail.com

The work developed a modification of the algorithm for detecting cloning of frames in video sequences. It is impossible to imagine the life of a modern person without the constant presence of digital technologies in it. They have become an integral part of our daily life. Everyone has a smartphone, almost everyone owns a personal computer or laptop. Photo and video recording technologies, as well as the distribution and publication of images and videos, such as social networks, have become an integral part of digitalization. Digitization has also spread to very important areas for human life, such as forensics or mass media. In order to have confidence in video materials, which is extremely important in criminal investigations, court cases and information networks, it is necessary to develop the field of exposing modifications and falsifications in video and photo materials, develop new methods that allow you to verify the integrity of the video or detect falsification, and modify and improve already developed ones. The paper analyzes the methods for finding falsifications in video sequences and modern formats and algorithms for saving and compressing video sequences. As a result of the analysis, the current state of development in the field of detection of fake videos was revealed and the most popular video formats were determined. Experiments were conducted with videos of different formats and resolutions, data were collected and analyzed, after which the necessary threshold values of the Pearson correlation coefficient were established for each format studied. Threshold values for searching for cloned frames were proposed in the work. The threshold value is chosen depending on the format and resolution of the video. Parameters such as video format and resolution were taken to modify the algorithm for detecting cloning of frames in a video sequence by analyzing the threshold values of the Pearson correlation coefficient. A software implementation of the modification of the algorithm for detecting cloning of frames in video sequences was created. Errors of the first and second kind are cited in the work.

Keywords: digital video, frame cloning, correlation coefficient, frame cloning detection.

DOI 10.15276/imms.v13.no3-4.266
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 266-274

МЕТОД ВИЯВЛЕННЯ ФІШИНГОВИХ QR-КОДІВ ІЗ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ

А.В. Касаяні, Н.І. Кушніренко, О.В. Троянський, В.В. Подуфалов

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mail: infsec2011@gmail.com

На сьогоднішній день існує багато інструментів, які можуть виявляти та блокувати шкідливі посилання, які ведуть до фішингових сайтів або зловмисного програмного забезпечення. Проте більшість з них поки не здатні перевіряти шкідливі QR-коди, і це дає зловмисникам можливість активно використовувати їх в атаках. Фішинг з використанням QR-кодів дуже схожий на інші форми фішингу. Ця атака спрямована на маніпулювання користувачами та отримання від них особистої інформації, такої як облікові дані для входу чи фінансова інформація. Суть фішингу з використанням QR-кодів не нова. Основна відмінність полягає в тому, що в цьому випадку QR-код використовується для перенаправлення жертви на шкідливий веб-сайт. Метою даної роботи є підвищення безпеки користувачів у цифровому середовищі шляхом розробки та впровадження методу виявлення фішингових QR-кодів з використанням машинного навчання. У роботі проведено аналіз методів та засобів протидії фішингу та атакам через QR-коди, який дозволив визначити напрямки розробки та основні завдання дослідження. Розроблений метод включає в себе аналіз особливих ознак посилання та його тексту за допомогою мовно моделі, на основі яких навчався та тестувався алгоритм машинного навчання. Створений метод виявлення фішингових QR-кодів значно підвищує безпеку користувачів у використанні QR-кодів. Аналіз ефективності розробленого методу показав результат у понад 90% точності виявлення. Метод виявлення фішингових QR-кодів, розроблений у рамках цієї роботи, може бути успішно впроваджений в діяльність різних організацій, включаючи підприємства та установи. Цей метод надає можливість зменшити ризики фішингових атак через QR-коди, що призводить до підвищення безпеки для співробітників. Результати даної роботи можуть бути використані при подальших дослідженнях, розробках у сфері кібербезпеки та боротьби з фішинговими атаками через QR-коди.

Ключові слова: фішинг, QR-код, машинне навчання, кібербезпека, мовна модель.

Вступ. Питання фішингу в сучасному інтернет-середовищі визначається як одна з найбільш поширених та серйозних загроз для безпеки користувачів та організацій. Фішинг є методом соціальної інженерії, який заснований на обмані та маніпуляціях з метою здобуття конфіденційної інформації, фінансових ресурсів або доступу до цифрових активів.

Особливу увагу слід звернути на фішингові атаки, які використовують QR-коди. Зараз QR-коди широко використовуються у рекламі, маркетингу та логістиці, і ця популярність робить їх привабливими для зловмисників. Вони можуть створювати фішингові QR-коди, які виглядають легітимними, але насправді ведуть до шахрайських веб-сайтів або завантажують шкідливе програмне забезпечення на пристрої користувачів.

Використання фішигових QR-кодів стало серйозним викликом для кібербезпеки і призвело до поганих наслідків для багатьох людей та компаній. Ось деякі відомі приклади цих атак [1]:

– паркувальні квитки у Китаї: У Китаї шахраї розміщали підроблені паркувальні квитки з QR-кодами на автомобілях. QR-коди надавали зручну можливість оплати за допомогою мобільних телефонів. Однак, фактично, це були шахрайські схеми, що призводили до фінансових втрат;
– мобільний банкінг в Нідерландах: У Нідерландах зловмисники використовували легальні функції мобільних банківських додатків для обману клієнтів. Вони використовували QR-коди, щоб провести фішингові атаки та вимагали конфіденційну інформацію;
– фальшиві електронні листи в Німеччині: У Німеччині злочинці використовували QR-коди у фальшивих електронних листах, щоб вести клієнтів системи електронного банкінгу на шкідливі веб-сайти, прикидаючись перевіркою політики конфіденційності;
– фішингові атаки в Техасі: В Техасі зловмисники приклеювали шкідливі QR-коди до міських паркоматів. Жертви, скануючи ці коди, потрапляли на фейкові фішингові сайти і вводили свої кредитні картки, стаючи об'єктом фінансового шахрайства.

Ці приклади свідчать про різноманітність атак, які використовують QR-коди для здійснення злочинних дій. З цим явищем пов'язані серйозні загрози для інтернет-безпеки, і важливо бути обережними при взаємодії з QR-кодами, особливо якщо вони надійшли від невідомих джерел. Це робить проблему фішингу через QR-коди актуальною та вимагає розробки ефективних методів виявлення цих атак.

На теперішній час існує багато методів для виявлення фішингових посилань, які використовують машинне навчання [2 - 4]. Вони мають високий рівень ефективності, але не пропонують боротьбу з фішинговими атаками через QR-коди, які все частіше становляться загрозою для підприємств та окремих користувачів. Тому було вирішено розробити метод, що застосовується саме для виявлення фішингу у QR-кодах. Розроблений метод містить у собі механізм аналізу тексту посилання за допомогою мовної моделі. Його ефективність порівняна або навіть перевищує ефективність інших методів.

Мета і задачі дослідження. Метою даної роботи є підвищення безпеки користувачів у цифровому середовищі шляхом розробки та впровадження методу виявлення фішингових QR-кодів з використанням машинного навчання. Для досягнення поставленої мети необхідно розв'язати такі завдання:

– аналіз предметної області – вивчення методів та засобів протидії фішингу, зокрема в контексті використання QR-кодів;
– розробка теоретичної основи виявлення фішингових QR-кодів;
– вибір методу машинного навчання;
– реалізація та тренування моделі машинного навчання для виявлення фішингових QR-кодів;
– тестування розробленого методу та аналіз ефективності.

Основна частина. Фішинг – це вид кіберзлочинності, який спрямований на отримання конфіденційної інформації від користувачів Інтернету шляхом імітації довірливих джерел або осіб [5]. Фішингові атаки спираються на соціальну інженерію та мають на меті обман цільових користувачів для отримання їхніх особистих даних, таких як паролі, номери кредитних карт та іншої фінансової інформації.

Соціальна інженерія відіграє ключову роль у фішингу, оскільки вона визначає ефективність атаки. В основі фішингу лежить психологічний вплив на жертву, який допомагає атакуючому переконати жертву надавати конфіденційну інформацію чи виконувати вказівки. Соціальна інженерія допомагає атакуючому створити обманливу ситуацію та надати вигляд довіри та легітимності атаки. Це може включати в себе імітацію офіційних логотипів, листів, повідомлень або веб-

сайтів, а також створення обманливих сценаріїв, які спонукають жертву до виконання дій на користь атакуючого [6].

Розглянемо основні види фішингу з якими можуть зіткнутися користувачі у Інтернет мережі [7 - 8]:

- фішинг через QR-коди (QR Code Phishing);
- голосовий фішинг (Vishing);
- фішинг через клонування (Clone Phishing);
- фішинг через соціальні мережі (Social Media Phishing);
- фішинг через смс-повідомлення (Smishing);
- фішинг через електронну пошту (Email Phishing);
- фішинг атака «злий двійник» (Evil Twin Phishing);
- китобійний фішинг (Whaling);
- цільовий фішинг (Spear Phishing).

QR-коди, або Quick Response Codes, є двовимірними штрих-кодами, які стали надзвичайно популярними в останні десятиріччя. Вони забезпечують ефективний спосіб кодування і передачі інформації, і використовуються в різних сферах, від маркетингу до логістики та медицини. QR-коди створені для швидкого і зручного зчитування інформації за допомогою сучасних мобільних пристроїв. Вони мають специфічну структуру, що дозволяє кодувати багато типів даних, включаючи текст, веб-посилання, контактну інформацію, географічні координати та багато інших.

Інформація, що зберігається в QR-коді, може приймати різні форми, але найчастіше вона є простим веб-посиланням. Наприклад, в операційній системі iOS додаток «Камера» автоматично розпізнає QR-коди і пропонує відкрити веб-сторінку за посиланням, що в них міститься. Основна інформація, яку слід мати на увазі щодо QR-кодів, полягає в тому, що вони часто служать як звичайні посилання на веб-сторінки і це має важливий вплив на питання кібербезпеки.

QR-коди, як зручний і поширений спосіб передачі інформації, стали привабливим знаряддям для зловмисників, які прагнуть використовувати їх для фішингових атак. Процес функціонування таких атак представлений на рисунку 1.

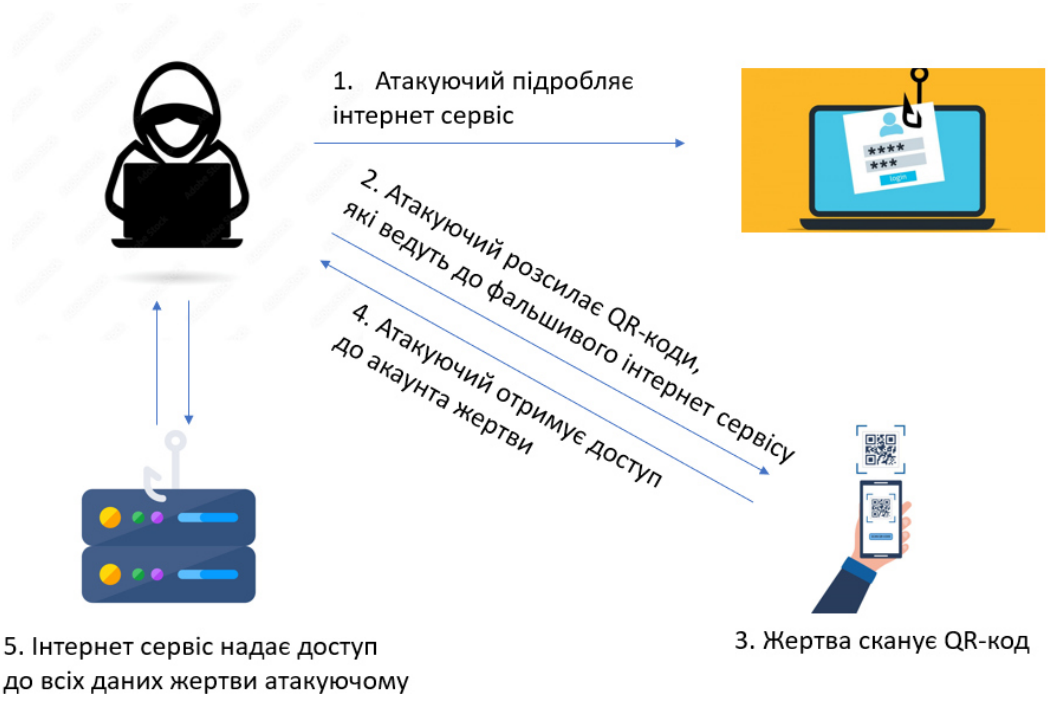


Рис.1. Фішингова атака із використанням QR-коду

QR-коди широко використовуються в різних галузях промисловості, спрощуючи процеси для торгівлі, розважальних закладів і ресторанів. Однак ця популярність не робить користувачів імунними до фішингових атак. Кіберзлочинці використовують QR-коди разом із обманливими повідомленнями, щоб змусити людей розголошувати конфіденційну та особисту інформацію. Підроблені QR-коди часто направляють жертв на фальшиві веб-сайти, де збираються конфіденційні дані, такі як номери кредитних карток. За допомогою цих викрадених даних хакери можуть отримати контроль над особою жертви і спричинити фінансовий хаос через несанкціоновані витрати з кредитної картки. Виявлення шкідливого QR-коду та захист від потенційних загроз надзвичайно важливі в цифровому середовищі.

Коли йдеться про QR-коди, важливо розрізняти їх різновиди, такі як фізичний QR-код та цифровий QR-код, оскільки обидва можуть бути використані в атаках фішингу, але мають свої особливості. Поговоримо про кожен з типів більш докладно.

Фізичний QR-код представляє собою візуальний штрихкод, який можна надрукувати чи нанести на поверхню. Такі QR-коди можуть бути підробленими чи розміщеними на несподіваних об’єктах, викликаючи замішання та підвищуючи ймовірність виникнення фішингових сценаріїв. У випадку фізичного QR-коду прикладом атаки є наклеювання підроблених кодів на фізичні об’єкти, такі як паркомати або продукти у магазинах.

Цифровий QR-код, навпаки, зберігається та розповсюджується в електронному форматі але також може бути розпізнаний за допомогою камери смартфона або іншого пристрою. Цифрові QR-коди можуть використовуватися на шахрайських інтернет сторінках, у смс-повідомленнях або в листах електронної пошти, що намагаються імітувати легітимні повідомлення від банків чи відомих компаній.

Особливості обох видів QR-кодів свідчать про необхідність пильності та обережності користувачів при взаємодії з ними, особливо в ситуаціях, де може виникнути підозра щодо їхнього походження чи наміру. Ось декілька аспектів, які варто врахувати для виявлення шахрайських QR-кодів [9]:

- перевірка джерела;
- перевірка URL-адреси;
- дизайн QR-коду;
- наявність механізму автентифікація;
- наявність запиту конфіденційної інформації;
- наявність надмірно щедрих пропозицій;
- використання програм сканування QR-кодів із вбудованими функціями захисту від фішингових атак;
- використання антивірусів та іншого корисного програмного забезпечення для захисту від шахрайства;
- регулярне оновлення програмного забезпечення безпеки;
- використання двухфакторної автентифікації.

Також слід підкреслити вразливість компаній та корпоративних спільноти до фішингових атак. Зростаюча поширеність шахрайства через QR-коди підкреслює критичну потребу компаній у посиленні свого захисту. Підсумовуючи, зручність QR-кодів не повинна приховувати постійну загрозу фішингових атак. Підприємства мають активно навчати свій персонал, створюючи пильну корпоративну спільноту, здатну вчасно розпізнавати та запобігати шахрайству. Шляхом навчання з кібербезпеки та використання спеціалізованого програмного забезпечення, організації можуть ефективно захищати себе від потенційних небезпек, забезпечуючи постійну безпеку своїх операцій та даних.

Як було зазначено вище, у QR-кодах найбільш поширеною формою інформації є веб-посилання, яке часто використовується для спрощеного доступу до веб-ресурсів. Також, у контексті кібербезпеки, важливо зауважити, що аналіз цього посилання є критичним етапом у виявленні можливих фішингових атак, оскільки саме воно приховує шкідливий вміст, спрямований на шахрайські цілі. При ретельному аналізі структури та джерела посилання, можливо виявити потенційно небезпечні QR-коди та запобігти їх шкідливому впливу.

Першим етапом на шляху до виявлення фішингових QR-кодів є декодування посилання та його подальший аналіз. Для виявлення потенційних вразливостей або ознак фальшивості, необхідно ретельно розглянути всі частини посилання, яке міститься в QR-коді. Цей процес включає дослідження протоколу передачі даних, доменних імен, шляху до ресурсу, параметрів запиту та інших метаданих.

Особливі ознаки у веб-посиланнях є ключовими компонентами аналізу. Ці параметри дозволяють виявляти певні відмінності та характеристики, які є типовими для підозрілих або потенційно шкідливих посилань.

У таблиці 1 наведено перелік особливих ознак посилання, обраних для методу виявлення фішингу.

Таблиця 1

Особливі ознаки посилання

Особливі ознаки адресної строки	Кількість двійних скісних рисок «//»
	Наявність IP-адреси безпосередньо у посиланні
	Наявність символу собака «@»
	Довжина посилання
	Наявність букв не латинського алфавіту
	Використання захищеного протоколу
Особливі ознаки домену	Кількість днів до закінчення терміну дії домена
	Кількість днів з моменту реєстрації домену
	Наявність піддомену

Перейдемо безпосередньо до алгоритмів машинного навчання. Машинне навчання може включати розробку моделі, яка навчається на певних тренувальних даних та використовується для обробки даних з метою передбачення результату. Для даної задачі будемо розглядати та порівнювати дві моделі машинного навчання: нейронні мережі та дерева рішень.

Наступний крок це аналіз тексту посилання за допомогою мовної моделі. Мовні моделі представляють собою складні математичні або комп'ютерні структури, що навчаються розуміти та генерувати мовленнєві зразки. Їхньою основною метою є розуміння мови, виявлення закономірностей у тексті та здатність створювати нові мовні вислови. Ці моделі базуються на великій кількості даних – текстах, документах, великих корпусах мовленнєвих матеріалів.

Головним поняттям при обробці природної мови є векторні відображення. Векторні відображення – це числові представлення слів або текстових фрагментів у векторному просторі. Сутність векторних відображень полягає в тому, що вони є словами чи текстом у формі, зрозумілими для комп’ютера, в якій відображена семантична та синтаксична інформація. Вектори відображення розташовані у таких просторах, де схожі слова або фрази розміщені близько одне до одного, відображаючи їхні семантичні відносини. Це дозволяє створити систему класифікації, яка здатна виявляти вирази або ключові ознаки, що вказують на можливу загрозу кібербезпеці.

Таким чином з тексту посилання ми отримуємо його числове представлення у вигляді вектору, який далі буде використовуватися як додаткові вхідні дані для алгоритму машинного навчання.

Блок-схема загального алгоритму виявлення фішингових QR-кодів представлена на рисунку 2.

Глибокий аналіз створеного методу виявлення фішингових QR-кодів спрямований на оцінку його ефективності. Він включає докладний аналіз результатів тестування, що охоплює точність та надійність новаторського підходу до виявлення підроблених QR-кодів. Мета цього аналізу – визначити потенційні можливості та обмеження запропонованого методу в контексті протидії фішинговим атакам.

Ефективність моделей у машинному навчанні, особливо в задачах бінарної класифікації, часто оцінюється за допомогою матриці помилок (Confusion Matrix). Ця матриця – ключовий інструмент для подальшої оцінки моделі, що дозволяє визначити різні показники, такі як точність, чутливість, специфічність та інші.

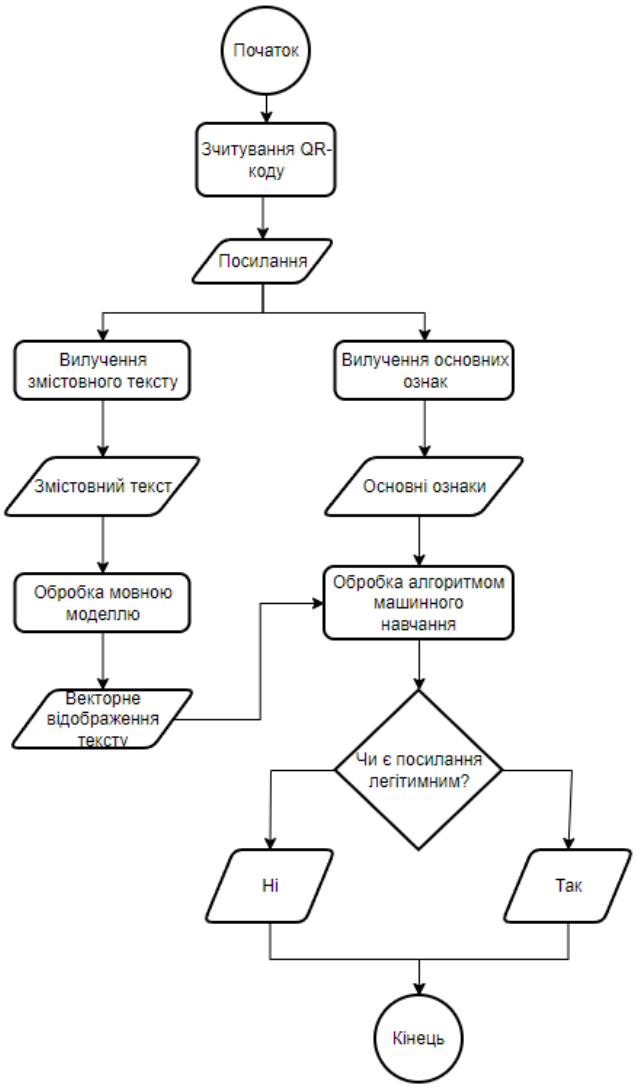


Рис.2. Блок-схема алгоритму аналізу QR-коду на предмет фішингу

Для обраних алгоритмів машинного навчання були розраховані матриці помилок, які у виді діаграм представлені на рисунку 3. Набір даних складався з 50000 посилань, з яких випадково обрані 70% були використані для тренування, а решта для тестування. Перші розрахунки були отримані лише з використанням аналізу особливих ознак посилання. При подальшій розробці алгоритму було

вирішено впровадити мовну модель, яка значно підвищила ефективність розпізнавання.

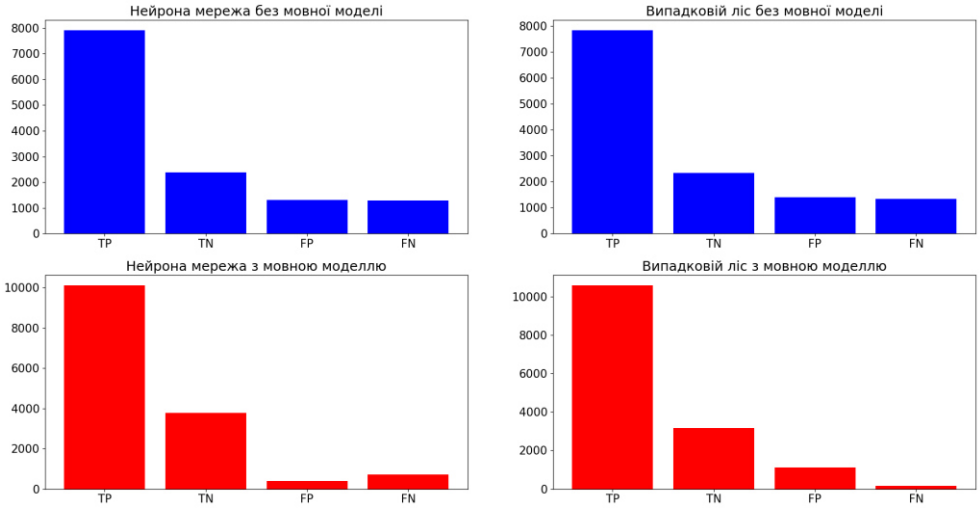


Рис.3. Діаграми значень матриці помилок

Отримавши матрицю помилок, ми переходимо до розрахунків ключових метрик ефективності моделі в бінарній класифікації. Зазвичай на основі цієї матриці визначаються такі показники, як [10]:

- точність (accuracy);
- влучність (precision);
- повнота (recall);
- специфічність (specificity);
- F-міра (F-score).

Кожен з цих показників відображає різні аспекти ефективності моделі в контексті конкретного завдання класифікації. Аналіз цих метрик надає глибше розуміння того, як добре модель пристосовується до розпізнавання певних класів, а також дозволяє здійснити порівняння з іншими моделями чи підходами до вирішення задачі.

Для розрахування цих метрик використовують наступні формули [10]:

$$Acurracy = \frac{TP + TN}{TP + TN + FP + FN},$$

$$Precision = \frac{TP}{TP + FP},$$

$$Recall = \frac{TP}{TP + FN},$$

$$Specificity = \frac{TN}{TN + FP}.$$

Після розрахунку основних метрик, таких як точність, влучність чутливість та специфічність, можна розрахувати F-міру (F-score). F-міра є комбінованою метрикою, що об’єднує влучність і чутливість моделі в одне числове значення. Формула розрахунку F-міри [10]:

$$F\text{-}score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Ця метрика надає комплексну оцінку ефективності моделі, враховуючи як правильність класифікації позитивних прикладів (чутливість), так і уникнення помилкових класифікацій позитивних та негативних прикладів (точність). Цей показник допомагає здійснити більш об’єктивне порівняння моделей та визначити їхню загальну ефективність у вирішенні задачі класифікації.

Для оцінки ефективності розробленого методу були побудовані графіки які відображають значення всіх вище перерахованих метрик ефективності. У рамках поставленої задачі розпізнавання фішингових QR-кодів ці графіки відображають порівняльну характеристику як алгоритмів машинного навчання так і самого методу до та після впровадження мовної моделі. Результати аналізу за метриками ефективності представлені на рисунку 4.

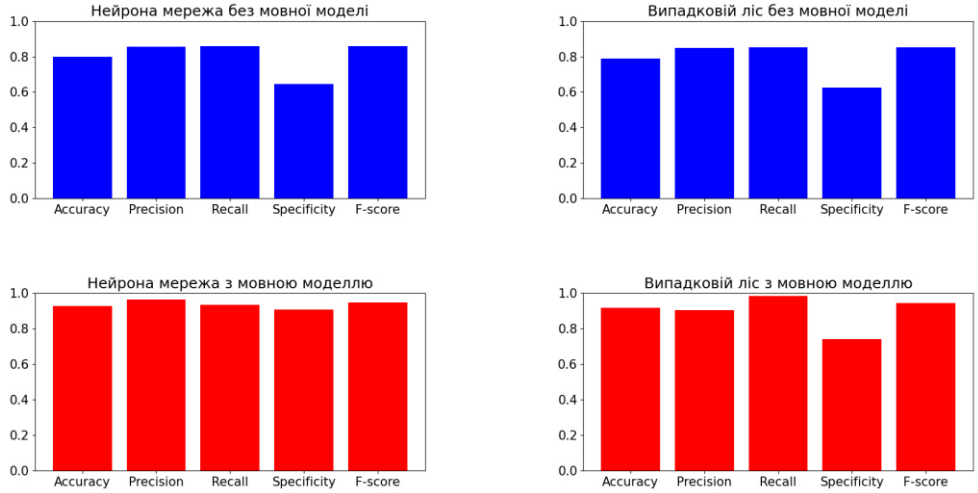


Рис.4. Діаграми значень метрик ефективності

Висновки. В роботі проведено аналіз фішингу та засобів для його виявлення та запобігання, а також надано важливе уявлення про загрозу, яку це питання складає у сучасному цифровому світі.

Розроблено метод виявлення фішингу в QR-кодах, який базується на аналізі особливих ознак посилання та його контенту з використанням технологій машинного навчання та мовних моделей. Проведено аналіз ефективності запропонованого методу. Отримані результати дають понад 90% точності у виявленні фішингових QR-кодів. Аналіз особливих ознак посилань, зокрема параметрів URL-адрес, структури посилання, структури домену тощо, дозволив створити модель, яка з високою точністю розпізнає потенційні фішингові посилання. Також, аналіз текстової інформації з QR-кодів за допомогою мовних моделей дав змогу виявити відмінності у способі побудови фішингових текстів посилання.

Отже, це дослідження має важливе теоретичне та практичне значення. Розроблений метод може бути використаний для покращення безпеки користувачів при взаємодії з QR-кодами, а також впроваджений у захисне програмне забезпечення мобільних пристроїв або сервісів, що виявляють потенційно шкідливі посилання та QR-коди.

Список літератури

1. Cloudav. 11 типов фишинга и их примеры из реальной жизни. URL: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/
2. Mridha K., Hasan J., Ghosh A., Saravanan D. Phishing. URL Classification Analysis Using ANN Algorithm. *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies* (GUCON) URL:https://www.researchgate.net/publication/355861339_Phishing_URL_Classification_Analysis_Using_ANN_Algorithm
3. Bouijij H., Berqia A. Machine Learning Algorithms Evaluation for Phishing URLs Classification. *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT).*

URL:https://www.researchgate.net/publication/357813273_Machine_Learning_Algorithms_Evaluation_for_Phishing_URLs_Classification
4. Nagasunder R., Pawar B., Rao P. Detection of Phishing URL using Machine Learning. 2021. URL: https://norma.ncirl.ie/5100/1/nagasunderraopawarbaburaopawar.pdf
5. Termin. Фішинг — що це таке, суть, визначення, види та приклади фішингу. URL: https://termin.in.ua/fishynh/
6. Radiosvoboda. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. URL: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html
7. Trendmicro. What Are the Different Types of Phishing. URL: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
8. Adlam S. Hidden Scams: Could QR Code Actually Be a Phishing Attack URL: https://gridinsoft.com/blogs/qr-code-phishing-attack/
9. Loyality company. How To Protect Your Business From QR Code Phishing Attacks. URL: https://www.linkedin.com/pulse/how-protect-your-business-from-qr-code-phishing-attacks/
10. Geeksforgeeks. Confusion Matrix in Machine Learning. URL: https://www.geeksforgeeks.org/confusion-matrix-machine-learning/

METHOD FOR DETECTING PHISHING QR CODES USING MACHINE LEARNING

A. Kasaiani, N. Kushnirenko, O. Troyanskiy, V. Podufalov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
e-mail: infsec2011@gmail.com

Today, there are many tools that can detect and block malicious links that lead to phishing sites or malware. However, most of them are not yet capable of validating malicious QR codes, and this gives attackers the opportunity to actively use them in attacks. Phishing using QR codes is very similar to other forms of phishing. This attack aims to manipulate users and obtain personal information from them, such as login credentials or financial information. Essence of phishing using QR codes is not new. The main difference is that in this case, a QR code is used to redirect the victim to a malicious website. The purpose of this work is to increase the security of users in the digital environment by developing and implementing a method for detecting phishing QR codes using machine learning. The work analyzed the methods and means of countering phishing and attacks through QR codes, which made it possible to determine the directions of development and the main tasks of the research. Developed method includes the analysis of special features of the link and its text using a language model, on the basis of which the machine learning algorithm was trained and tested. The created method of detecting phishing QR codes significantly increases the safety of users in the use of QR codes. Analysis of the effectiveness of the developed method showed a result of more than 90% detection accuracy. The method of detecting phishing QR codes, developed within the framework of this work, can be successfully implemented in the activities of various organizations, including enterprises and institutions. This method provides an opportunity to reduce the risks of phishing attacks through QR codes, resulting in increased security for employees. The results of this work can be used in further research, development in the field of cyber security and combating phishing attacks through QR codes.

Keywords: phishing, QR code, machine learning, cybersecurity, language model.

DOI 10.15276/imms.v13.no3-4.275
УДК 004.9

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 275-281

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗБЕРІГАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

О.Р. Осколкова, В.В. Зоріло

Національний університет “Одеська політехніка”
1 Шевченка пр., Одеса, 65044, Україна
e-mail: vikazorilo@gmail.com

У сучасному світі дуже часто постає питання щодо збереження та захисту парольних даних. Існує чимало сервісів та інтернет-ресурсів, до яких потрібно мати певні доступи, аби потрапити до системи. Коли ресурсів і паролів багато, то виникає питання, де і в якій формі їх зберігати. Зазвичай для цього використовують програмні рішення – менеджери паролів. *Мета* даної роботи полягає у підвищенні ефективності зберігання інформації з обмеженим доступом шляхом розробки додатку з можливістю шифрування. Для досягнення мети було проведено огляд та аналіз сучасних менеджерів паролів, який показав, що в повній мірі існуючі рішення не можуть задовольнити вимоги багатьох підприємств, зокрема, підприємства «OdesSeo», яке займається комплексним інтернет-маркетингом і знаходиться у місті Одеса. Для зберігання інформації з обмеженим доступом у зашифрованому вигляді було вибрано алгоритми шифрування SHA3 для паролів до акантів працівників, та AES-256 для паролів до проектів замовників послуг. Шифри останніх переводили у формат позиційної системи числення Base64. Розроблено мобільний додаток – менеджер паролів, який було успішно впроваджено у виробництво підприємства «OdesSeo». Підвищення ефективності зберігання інформації з обмеженим доступом на підприємстві «OdesSeo» вимірюється в грошовому еквіваленті, нижня межа якого складає 50000 грн або 1200$, що за оцінками ризик-менеджерів відповідає мінімально-необхідним витратам на усунення наслідків витоку інформації чи несанкціонованого доступу до системи підприємства та проектів клієнтів.
Ключові слова: менеджер паролів, шифрування, захист інформації, кібербезпека.

Вступ. У сучасному світі дуже часто постає питання щодо збереження та захисту парольних даних. Існує чимало сервісів та інтернет-ресурсів, до яких потрібно мати певні доступи, аби потрапити до системи. Коли ресурсів і паролів багато, то виникає питання, де і в якій формі їх зберігати. На даний момент існують рішення, які закривають дане питання, але в них є деякі недоліки та особливості. Часто повний функціонал додатків можливо використовувати тільки за умовою придбання ліцензії, особливо у випадку використання у виробництві. Для великих компаній ця сума може сягати десятків і навіть сотень тисяч доларів. Також не завжди розробники менеджерів паролів мають хорошу репутацію: багато з них не вийшли з російського ринку та продовжують співпрацювати з країнами-терористами, що знижує довіру до них. Ці та інші причини спонукають компанії та підприємства шукати власні рішення для збереження такого виду інформації з обмеженим доступом, як паролі, ключі до шифроалгоритмів тощо.

Мета роботи полягає у підвищенні ефективності зберігання інформації з обмеженим доступом шляхом розробки додатку з можливістю шифрування.

Для досягнення поставленої мети необхідно вирішити наступні *задачі:*

1) огляд та аналіз сучасних рішень;

2) визначення методів зберігання інформації з обмеженим доступом;

3) розробка проекту програмного додатку;

4) реалізація програмного додатку.

Для конкретики будемо вирішувати дані задачі для підприємства «OdesSeo», не обмежуючи при цьому можливість адаптації і використання розробки для інших підприємств.

Основна частина. Підприємство «OdesSeo» займається комплексним інтернет-маркетингом, знаходиться у місті Одеса, існує на ринку вже 10 років і є лідером у своїй сфері. Послуги, які надає компанія, наступні: розробка сайтів – створення дизайну сайту, написання основного функціоналу сайту на основі розробленої CMS (розробка компанії); seo-просування та seo-оптимізація сайту; створення та реалізація комплексної маркетингової стратегії для просування бізнесу клієнта он-лайн; контекстна реклама (PPC) та реклама у соціальних мережах (SMM).

До цієї компанії звертаються різні бізнеси за послугами. Кожний бізнес має власні доступи до різних систем, сайтів, сервісів. Всі необхідні доступи бізнес має надати компанії для подальшої роботи. Ці доступи надаються певним співробітникам компанії, не усім, а тільки тим, хто буде працювати над проектом. Також варто враховувати, що в кожного співробітника є власні доступи, наприклад: корпоративна пошта, робочі акаунти в соціальних мережах і тому подібне.

Уся перелічена інформація є інформацією з обмеженим доступом. В тому числі від забезпечення її конфіденційності, цілісності та доступності будуть залежати ефективність роботи підприємства та його клієнтів і партнерів, репутація підприємства, прибутки та інші важливі для підприємства показники. Тому компанія зацікавлена в надійності додатку для зберігання даної інформації.

Додаток повинен задовольняти наступним вимогам: можливість створення акаунту для кожного співробітника; можливість створення записів з паролями та інформацією про проекти у власному акаунті співробітника; можливість поділитися паролем/паролями проектів з іншим співробітником; двохфакторна автентифікація працівника; шифрування паролю для входу в акаунт; шифрування паролів проектів, які зберігаються у додатку. Також дуже важливою та принциповою вимогою є те, що компанія-розробник відповідного менеджера паролів не повинна співпрацювати з компаніями РФ.

Розглянемо наступні рішення [1-5].

LastPass. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та переваги додатку: 256-бітове шифрування AES; PBKDF2 SHA 256 та хешування з додаванням «солі»; автоматичне заповнення паролів; редагування пароля; генератор паролів; безпечний пароль і спільний доступ до нотаток; пошук паролем або сайтом; масове додавання та збереження паролів; система авторизації. Недоліки: базові установки генератора паролів менш захищені; висока вартість ліцензії. Не вийшли з російського ринку.

Dashlane. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: автоматичне заповнення паролів; масове додавання та збереження паролів; 256-бітове шифрування AES; генератор паролів; можливість внесення додаткової інформації щодо збережених паролів; система авторизації; можливість редагування паролів; хмарний контейнер; автоматичний контроль термінів старіння паролів; надсилання повідомлень про необхідність змінити дані для доступу; можливість встановити новий персональний пароль. Недоліки: висока вартість ліцензії; «хмарний» контейнер доступний тільки у платній версії; додаток має відкритий код, будь-хто може проаналізувати цей код та виявити вразливості.

1Password. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: висока надійність; наявність вбудованого генератора паролів; можливість створення резервних копій; гібридне AES-шифрування з 128

або 256 бітною маскою; зберігання та редагування паролів; зберігання додаткової важливої інформації. Програма зберігання паролів 1Password дозволяє підключатися до комп'ютера віддалено. Синхронізує пристрої за допомогою єдиного облікового запису на смартфонах та ПК. Недоліки: висока вартість; немає можливості обмінюватися даними з користувачами; якщо не оплатити підписку, то користувач більше не матиме доступу до своїх старих паролів.

Bitwarden. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: багатофакторна автентифікація; 1гб зашифрованого файлового сховища з преміям-планами; синхронізація з хмарою; наскрізне шифрування AES 256 біт, хешування та PBKDF2 SHA-256; можливість писати та виконувати сценарії у сховищі Bitwarden. Недоліки: додаток має відкритий код.

Keeper. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: персональне сховище для кожного користувача; автоматичне заповнення паролів; кількість даних, які можна зберігати у додатку, не обмежуються; генерація паролів; підтримка імпорту даних з інших менеджерів паролів та можливість експорту до PDF, CSV або JSON. Недоліки: складна процедура відновлення доступу до облікового запису, є можливість втрати даних; висока вартість обслуговування; не вийшли з російського ринку.

Для зручності порівняння існуючих рішень скористаємося таблицею 1.

Таблиця 1

Порівняльний аналіз існуючих аналогів

Функції	Назва мобільного додатку				
	LastPass	Dashlane	1Password	Bitwarden	Keeper
Шифрування даних	+	+	+	+	+
Система авторизації	+	+	+	+	+
Збереження та редагування паролей	+	+	+	+	+
Створення резервних копій	-	-	+	-	+
Внесення додаткових коментарів	+	+	+	-	-
Генератор паролів	+	+	-	-	-
Можливість ділитися парольними записами	-	-	-	-	+
Зручний та простий інтерфейс	-	+	+	-	+
Сучасний дизайн	-	+	+	+	+
Автономність	-	+	-	+	+
Вийшли з російського ринку	-	-	+	-	-
Вартість ліцензії на місяць на одного користувача	$10,20	Від $10	$19,95*	$20*	$45

* залежить від кількості людей

Як можемо бачити, жоден із додатків не задовольняє в повній мірі висунутим вимогам. Враховуючи важливість даних, які необхідно захистити, розробимо власне програмне забезпечення.

Для коректної роботи підприємства «OdesSeo» необхідно безпечно зберігати доступи кожного клієнта та передавати їх між співробітниками, що працюють над спільними проектами, а саме доступи до сайтів, хостингу, акаунтів соціальних мереж тощо. Втрата або витік цієї інформації на підприємстві може призвести до небажаних наслідків, матеріальних та репутаційних збитків.

База даних буде складатися з наступних таблиць: «User» для зберігання та реєстрації даних для ідентифікації, аутентифікації та авторизації працівників; «Passwords» для зберігання записів користувача, які є інформацією, наданою клієнтами/партнерами; «Receivepass» для записів про те, хто з працівників поділився паролем та з ким, і про його статус – «прочитано»/«не прочитано» (рис.1).

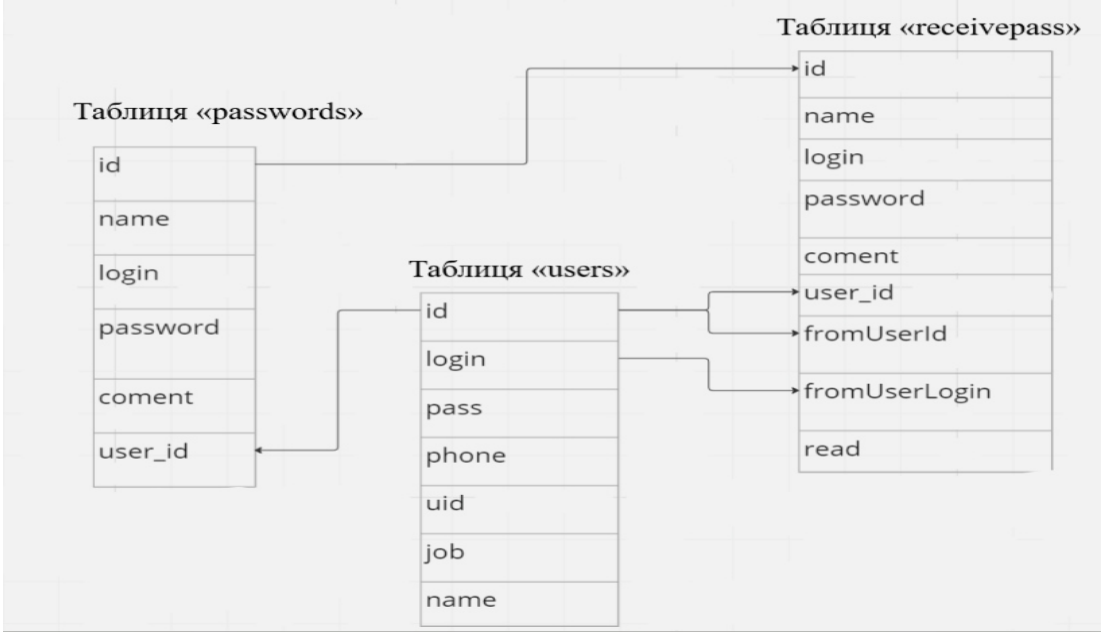


Рис. 1. Схема бази даних для серверної частини додатку

Безпека процесу реєстрації та авторизації користувачів в системі забезпечується шляхом шифрування пароля для входу в обліковий запис. Шифрування здійснюється на серверній стороні, зашифровані дані зберігаються у таблиці «User».

Для паролів працівників встановимо наступні обмеження: довжина повинна бути не менше 10 символів, пароль повинен містити хоча б одну велику літеру, хоча б одну цифру і хоча б один спеціальний знак з наступного переліку знаків {!, ?, %, &}; алфавіт має складатися з латинських літер, арабських цифр та спеціальних знаків, потужність алфавіту з врахуванням регістрів складає 66 символів. Таким чином для підбору одного символу пароля можливі 66 варіантів, а кількість усіх можливих комбінацій складає 66^{10}.

З міркувань безпеки паролі на сервері будуть зберігатися у вигляді хешу, згенерованого засобами алгоритму SHA3. До пароля при шифруванні буде додаватись «сіль». Разом з іншими даними про працівника пароль потрапляє на сервер, де створюється новий запис у таблиці «Users».

Для додаткового захисту використаємо двохфакторну автентифікацію, де другий фактор захисту буде реалізовано через корпоративний номер телефону працівника: для авторизації чи реєстрації користувачів необхідно отримати підтвердження у вигляді коду, який буде надіслано як SMS-повідомлення на вказаний номер телефону. При реєстрації код надсилається лише у випадку, якщо користувача ще немає у системі. При авторизації код відправляється тільки у випадку, якщо вказаний користувач вже зареєстрований у системі.

Під час роботи з проектами замовників послуг працівники «OdesSeo» створюють у застосунку записи про клієнтів з наступною інформацією: назва проекту, логін, пароль та коментар для конкретного запису. Ці дані зберігаються у базі даних у таблиці «Passwords». Пароль також зберігається у зашифрованому вигляді. Шифрування відбувається на пристрої працівника ще до того, як

відправити їх до бази даних.

При створенні працівником запису про клієнта поле з паролем проекту шифрується алгоритмом симетричного шифрування AES-256 за допомогою унікального для кожного проекту ключа шифрування, що зберігається у файлах додатка та разом з іншими даними відправляється до бази даних. Ключ зберігається в базі даних у таблиці «passwords» зашифрованому вигляді.

Для того, щоб розшифрувати пароль, необхідно щоб користувач у полі для вводу ввів власний ключ шифрування (рис. 2). Не знаючи ключ шифрування, побачити пароль в дешифрованому вигляді не можливо.

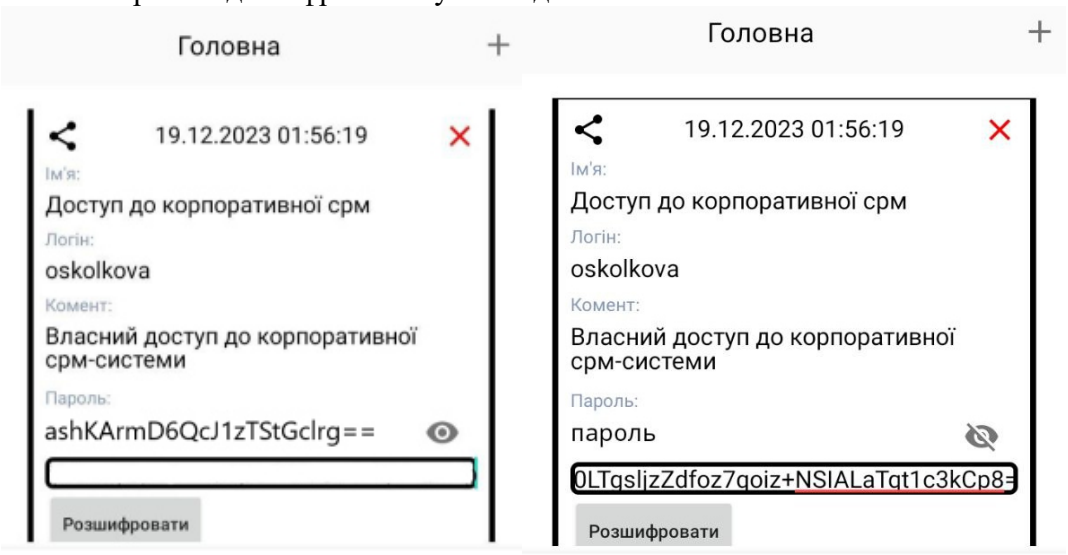


Рис.2. Дешифрування паролю

Процес генерації ключа шифрування було удосконалено шляхом додавання логіну користувача та конвертації ключа з шифру AES-256 у представлення в позиційній системі числення Base64. Обрана комбінація симетричного шифрування пароля з додаванням логіна працівника та солі та представлення шифру у Base64 забезпечує достатній рівень безпеки, прийнятну швидкість шифрування, ефективність та зручність в роботі з ключем шифрування.

Можливість поділитися парольним записом з іншим працівником в застосунку реалізовано у вигляді функції вибору конкретного працівника та передачі конкретного запису з паролем. В таблиці «Receivepass» при цьому буде створено запис з інформацією про: проектну назву, логін, пароль та коментар; ідентифікатор та логін відправника; ідентифікатор отримувача; статус запису «прочитано»/«не прочитано».

Під час реєстрації працівнику надається можливість заповнити спеціальну форму, яка включає наступні поля: прізвище; ім'я; по-батькові; логін; номер телефону; посада в компанії; пароль. Після заповнення форми та натискання кнопки «Зареєструватися» дані відправляються на сервер для перевірки наявності в базі даних. Якщо збіг знайдений, користувач отримує повідомлення про існуючий акаунт і неможливість реєстрації з заданими параметрами. Інакше система переходить до наступного етапу – перевірка за вказаним номером телефону – надсилання повідомлення з кодом підтвердження (рис. 3), відсіювання ботів через проходження капчі (рис. 4).

В результаті успішного проходження останнього етапу створюється новий запис у базі даних з інформацією про працівника та його унікальним ідентифікатором. Ці заходи значно підвищують рівень безпеки реєстрації та збереження даних користувачів у системі.

Авторизація працівника передбачає введення даних: логін, номер

телефону, пароль, унікальний ключ для шифрування, який зберігається на пристрої користувача. Після заповнення всіх полів пароль піддається хешуванню з сіллю, що дозволяє зменшити ризики атак з використанням «райдужних таблиць», відбувається пошук отриманого хешу на сервері. Якщо запис знайдено, користувач авторизується в системі. Інакше відбувається відмова в авторизації, а після певної кількості невдалих спроб – блокування акаунта. Це дозволяє протистояти можливій атаці перебору паролів «грубою силою».

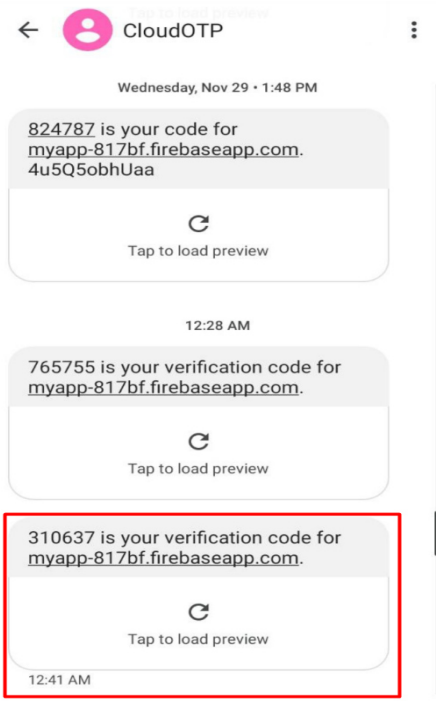


Рис.3. Надсилання повідомлення з кодом підтвердження

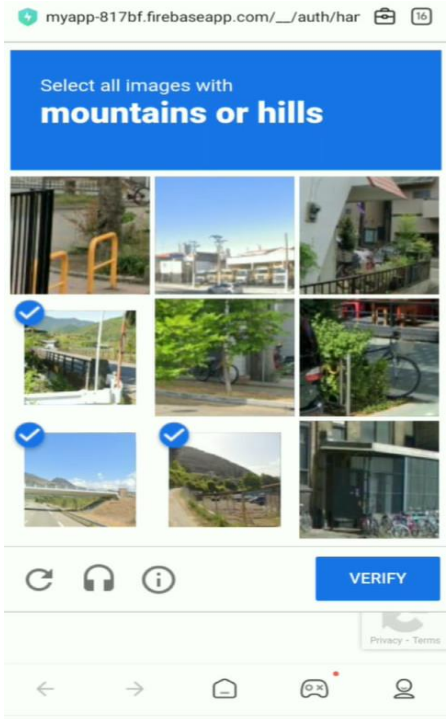


Рис. 4. Приклад проходження капчі

Для виводу на сторінці працівника доступних йому проектних записів система за ідентифікатором працівника створює запит до бази даних до таблиці «Passwords» та повертає дані, що належать користувачеві. Він може їх видаляти, редагувати, створювати нові, або надсилати їх колезі. Пароль доступу до проекту буде відображатись у зашифрованому вигляді. Для розшифрування необхідно ввести ключ.

Одночасно з цим на пристрої працівника-відправника виконується генерація ключа шифрування, що буде використовуватися для шифрування і дешифрування паролів, які користувач буде створювати і зберігати у додатку.

Для того, щоб поділитися паролем, необхідно обрати запис з паролем та існуючого користувача зі списку. Отримані доступи від інших користувачів зберігаються в окремому вікні, де можна побачити запис з паролем та від кого був отриманий запис. Для дешифрування отриманих записів необхідно отримати ключ того працівника-відправника. Згідно встановленої на підприємстві політики безпеки даний ключ можна отримати за оформленим запитом до адміністратора, який має схвалити керівник проекту.

Висновки. Проведено огляд та аналіз сучасних рішень збереження паролів, в результаті якого виявлено, що існуючі менеджери паролів попри свої переваги мають ряд недоліків, які для конкретних підприємств можуть виявитись неприпустимими та спонукати до розробки власних рішень.

Дану роботу було виконано для підприємства «OdesSeo», яке займається комплексним інтернет-маркетингом і яке потребує особливої уваги у питанні

збереження паролів.

Розроблено програмний додаток – менеджер паролів. Основним функціоналом програмного додатку є реєстрація, авторизація користувачів, можливість створювати та ділитися парольними даними і захист паролів від атак зловмисників. Переваги розробленого застосунку у порівнянні з існуючими аналогами полягають у вдосконалені процесу генерації ключа шифрування для паролів, що зберігаються у додатку, шляхом додавання логіну користувача та конвертації шифру ключа, виконаного алгоритмом AES-256, до виду позиційної системи числення Base64. Паролі доступу до акантів працівників зберігаються на сервері у вигляді хешу. Хешування відбувається алгоритмом SHA3 з додаванням солі.

Підвищення ефективності зберігання інформації з обмеженим доступом на підприємстві «OdesSeo» вимірюється в грошовому еквіваленті, нижня межа якого складає 50000 грн або 1200$, що за оцінками ризик-менеджерів відповідає мінімально-необхідним витратам на усунення наслідків витоку інформації чи несанкціонованого доступу до системи підприємства та проектів клієнтів.

Список літератури

1. Ahlgren M. Lastpass VS Dashlane (Password Manager Comparison). URL: https://www.websiterating.com/password-managers/lastpass-vs-dashlane/
2. Усама З. 5 найкращих менеджерів паролів для Windows в 2024. URL: https://uk.wizcase.com/blog/найкращі-менеджери-паролів-для-windows/
3. Шевченко Л. П’ять найкращих менеджерів паролів для вашої безпеки. URL: https://processer.media/ua/pass-managers/
4. Гарг Д. Огляд Keeper Password Manager 2023: чи він найкращий для керування паролями та секретами? URL: https://jitendra.co/uk/keeper-password-manager-review/

ENHANCING THE EFFICIENCY OF STORING RESTRICTED INFORMATION

O.R. Oskolkova, V.V. Zorilo

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044
email vikazorilo@gmail.com

In the contemporary world, there is a frequent concern regarding the preservation and protection of password data. Numerous services and internet resources require specific accesses to enter their systems. When dealing with a multitude of resources and passwords, the question arises as to where and in what form to store them. Typically, software solutions, namely password managers, are employed for this purpose. The objective of this study is to enhance the efficiency of storing restricted-access information by developing an application with encryption capabilities. To achieve this goal, a review and analysis of modern password managers were conducted, revealing that existing solutions fail to meet the requirements of many enterprises, including 'OdesSeo,' a comprehensive internet marketing enterprise located in the city of Odesa. For the secure storage of restricted-access information, SHA3 encryption algorithms were chosen for employee account passwords, while AES-256 was selected for project passwords of service clients. The latter ciphers were translated into Base64 positional numeral system format. A mobile password manager application was developed and successfully implemented in the production environment of 'OdesSeo.' The increase in the efficiency of storing restricted-access information at 'OdesSeo' is measured in monetary terms, with the lower threshold being 50,000 UAH or 1,200 USD, representing the minimum necessary expenses, according to risk managers' estimates, to mitigate the consequences of information leaks or unauthorized access to the enterprise system and client projects.

Keywords: password manager, encryption, information protection, cyber security.

DOI 10.15276/imms.v13.no3-4.282
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 282-292

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

П.Ю. Паталашко, Н.І. Кушніренко, Н.Г. Козаченко, Н.В. Бойко

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mail: infsec2011@gmail.com

У випадку, коли проблема виникає у мережі, IT-спеціалісти повинні бути впевнені, що будуть повідомлені про неї та отримають необхідну інформацію для її вирішення й виключення подібних ситуацій в майбутньому. Важливим елементом моніторингу мережі є сповіщення. Коли в мережі виникає аномальна поведінка, система повинна негайно повідомити IT-спеціалістів, щоб вони могли швидко реагувати. Саме тоді процес відновлення стану мережі стає найбільш ефективним. Моніторинг мережі в обов'язковому порядку повинен включати автоматичне отримання повідомлень про збої та події, які можуть впливати на продуктивність. У разі помилки, такі сповіщення мають бути надіслані через електронну пошту, SMS або інший зручний канал. Динамічні мережі вимагають систем, які могли б ідентифікувати вразливості в реальному часі. Тому деякі системи моніторингу мережі надають можливості для збору даних про безпеку, такі як мережеві журнали, журнали додатків та повідомлення про безпеку. Ці дані збираються та аналізуються для виявлення аномалій, і в разі появи загроз можливо надіслати сповіщення відповідному IT-спеціалісту. Таким чином, система моніторингу мережі дає можливість: забезпечувати неперервний робочий процес, відстежувати стан мережі та вчасно реагувати на можливі проблеми, поліпшувати ефективність роботи мережі, підвищувати надійність та безпеку мережі. Враховуючи це, можна зробити висновок, що для успішного функціонування мережі дуже важливо проводити їх моніторинг та вчасно реагувати на виникнення проблем. Для цього потрібно використовувати спеціалізовані системи моніторингу, які здатні швидко аналізувати стан мережі, визначати проблемні місця та повідомляти про них відповідних спеціалістів. Ця робота була зосереджена на аналізі наявних систем моніторингу мережі, висвітлено їх плюсів та мінусів. Досліджено технології та методики, що застосовуються для створення таких рішень. Розроблено нову систему моніторингу, спрямовану на оптимізацію процесу відстеження статусу мережевої безпеки. Збагачено функціонал системи відправкою сповіщень, а також впровадженням правил відстежування аномальної поведінки в мережі, що допоможе краще виділяти зловмисницькі дії та вчасно попереджувати спеціалістів.

Ключові слова: моніторинг, ELK-стек, OSSEC, ElastAlert, інцидент, логи, метрики.

Вступ. Коли підприємство розпочинає займатися питанням інформаційної безпеки, йому потрібно впровадити масу різноманітних систем. Це можуть бути антивірус, мережевий брандмауер, мережева та серверна системи виявлення вторгнень, міжсистемний фаєрвол, сканер уразливостей, система обліку цілісності, та багато іншого. Список інструментів, які можуть використовуватися в структурі, є досить широким. Оскільки безпека являє собою не лише стан системи (у традиційному розумінні), але й процеси, важливою складовою яких є моніторинг подій з інформаційної безпеки [1]. У будь-якому випадку виникає запитання про централізоване спостереження та аналіз журналів подій, які згенеровані перерахованими системами в різних масштабах.

На сьогоднішній день існує ряд рішень для організації моніторингу. Наприклад, вкрай популярним рішенням є Splunk. Цей інструмент збирає, індексує та співвідносить дані в реальному часі у сховищі з можливістю пошуку і виконання різноманітних запитів за заданими параметрами. За отриманими результатами можна створювати графіки, звіти, інформаційні панелі та різноманітні візуалізації [1]. Splunk має багато переваг, включаючи збір, відстеження, моніторинг та аналіз великих обсягів даних, які можна виконати в історичному режимі пошуку або в реальному часі. Проте він досить вартісний, особливо при великих обсягах даних, а його можливості створення власних правил кореляції обмежені у термінах складності та гнучкості.

Ще одне рішення для організації моніторингу, що було розглянуто – LogPoint [2]. Для даного інструменту можна відзначити вибір методу зберігання логів: залежно від цінності даних, ви можете вказати різні періоди зберігання, а також можливість створення складних кореляційних пошукових запитів. Крім того, можна налаштувати автоматичне сповіщення, використовуючи будь-який створений запит, що активує електронного листа при виявленні події. З недоліків LogPoint - недостатня інтуїтивна структура, яка ускладнює пошук деяких функцій. Хоча ціна на систему є доволі конкурентоспроможною, відсутність безкоштовної версії обмежує можливість її використання невеликими підприємствами. Спільнота користувачів LogPoint не є такою широкою і активною, як у інших пропозицій на ринку.

Іншим досить популярним рішенням є ELK-стек, що приваблює відкритим кодом, який дає можливість впровадити моніторинг будь-кому, незалежно від розміру компанії [3]. Це сприяє легкому впровадженню і гнучкості у налаштуванні системи для конкретних потреб організації. Недоліками даної системи є відсутність правил кореляції і механізму створення правил для відстежування характеру логів [4]. Також без додаткових компонентів в системі відсутній вбудований механізм сповіщення про потенційні загрози, його потрібно встановлювати окремо [5]. З іншого боку ELK-стек має суттєві переваги:

– ELK є безкоштовною системою (не зважаючи на витрати серверів). Попри вимоги витрат на налагодження та підтримку, вона забезпечує кращий баланс вартості і потужності;

– дозволяє збирати метрики, обробляти великі обсяги даних;

– відкритий код, що надає значну гнучкість у впровадженні;

– швидкість розгортування і легку масштабованість;

– має зручний API для створення запитів і можливості програмної інтеграції з іншими продуктами;

– добре розвинута спільнота користувачів, що забезпечує постійне оновлення та вдосконалення системи, а також швидке вирішення виникаючих проблем.

Беручи до уваги вищеописані недоліки і переваги, було вирішено розглянути потенційні способи подолання і збагачення функціоналу ELK-стеку для розробки власної системи моніторингу. В якості додаткових рішень з відкритим програмним кодом доцільно використати: Elastalert – для організації відстежування і відправки сповіщень, OSSEC – у якості елементу для конфігурації правил порушення безпеки.

Мета і задачі дослідження. *Метою роботи* є підвищення ефективності відстежування стану безпеки комп’ютерної мережі шляхом розробки системи моніторингу подій. За рахунок такого підходу підвищиться рівень безпеки організації, та значно знизиться час, що пройшов від моменту виникнення конкретних подій, до моменту їх нейтралізації. Альтернатив у відкритих джерелах

не було знайдено, що підвищує цінність розробки. В процесі виконання даної роботи необхідно розв'язати наступні задачі:

– проаналізувати та виявити найбільш важливі метрики для збору, що відображають стан мережі, а також найчастіші можливі порушення безпеки на серверах;

– обрати і описати складові частини для розробки системи моніторингу;

– розробити програмний продукт для візуалізації централізованого моніторингу комп'ютерної мережі.

Основна частина. Моніторинг мережі – процес відстежування дієздатності та стабільності мережі, її функціонування та продуктивності в рамках складних мережевих структур [6]. Він об'єднує процеси спостереження та аналізу мережевих компонентів таких, як роутери, комутатори та брандмауери, а також з'єднань між ними. Моніторинг мережі також охоплює керування різними рівнями даних, кінцевими мережевими вузлами та інтерфейсами.

Роутери, комутатори та вузли створюють сполучення між великою кількістю робочих станцій і ключовими програмними застосунками, розміщеними на численних серверах і в Інтернеті. Крім того, налаштовані безліч інструментів і застосунків безпеки та комунікацій, включаючи брандмауери, віртуальні приватні мережі (VPN), і антивіруси.

Перевірка роботи та продуктивності інтерфейсів стосовно їхніх потенційних збоїв сприяє діагностуванню, оптимізації і контролю різних мережевих ресурсів як локально, так і на відстані. За допомогою даних, представлених у вигляді таблиць, діаграм, графів, інформаційних панелей та звітів, моніторинг мережі дозволяє системним адміністраторам зменшити середній час відновлення (MTTR), а також розв'язати проблеми мережевої продуктивності в режимі реального часу. Коли подібні проблеми виявлені, система повідомляє системних адміністраторів безпосередньо або за допомогою підтримки, дозволяючи ним найшвидше розв'язати проблему.

Розуміння архітектури та складності мережі, обізнаність про роботу кожного її складового елемента у будь-який момент – все це важливі чинники, які сприяють успішному підтриманню стабільності та цілісності мережі компанії і її клієнтів. В мережі може бути тисячі точок даних для моніторингу, тому край важливим є доступ до значущої, точної та актуальної інформації в будь-який час. Системні адміністратори повинні постійно бути в курсі всього, що відбувається в кожному сегменті мережі.

Мережа, як правило, має внутрішніх та зовнішніх користувачів, включаючи співробітників, клієнтів, партнерів та інші сторони. Відмова мережі може мати різний ефект на бізнес, в залежності від типу користувача. Наприклад, якщо працівники не можуть отримати доступ до потрібної інформації для виконання роботи, це може призвести до зниження продуктивності, фінансових втрат і, ймовірно, шкоди репутації компанії в майбутньому.

Кожний компонент мережі є потенційною точкою відмови. Тому надзвичайно важливим є розроблення стратегії, що мінімізує можливість збою. Таким чином, якщо один сервер або роутер зазнає збою, інший може автоматично під'єднатися до мережі для зменшення ефекту від відмови головного обладнання. Не всі проблеми можуть бути прогнозовані й розв'язані до моменту, коли реальні загрози стануть очевидними. Але якщо здійснювати активний контроль мережі в режимі реального часу, можливо виявити та розв'язати проблеми до того, як вони набудуть глобальних обсягів. Наприклад, перевантажений сервер може бути замінений, перш ніж він зазнає збою, але це можливо лише при своєчасному отриманні цієї інформації.

Система моніторингу мережі може стати важливим інструментом для подальшого розвитку та планування мережі. Завдяки своїй здатності інформувати IT-спеціалістів про використання окремих елементів мережі та передбачати потенційні виклики, що можуть призвести до перевантаження, така система може сприяти ефективній адаптації мережі до швидкого зростання бізнесу або збільшення числа користувачів.

Інструменти моніторингу мережі забезпечують системному адміністратору постійний доступ до актуальної інформації про стан мережі, що дає можливість оперативно реагувати на виникнення проблем та вирішувати їх вчасно. Саме таким функціоналом володіє система, що буде лежати в основі рішення для моніторингу мережі. Як з'ясовано раніше, ELK-стек немає можливості відправки сповіщень і налаштування правил для аналізу записів у системних журналах. Тому далі буде детально описані рішення, що будуть використовуватися для доповнення функціоналу системи.

У якості рішення для відправки сповіщень було обрано легковісний ElastAlert. ElastAlert – це простий фреймворк для сповіщення про аномалії, сплески та інші патерни з даних в Elasticsearch [7]. Elastalert дозволяє створювати правила, які будуть описувати будь-які цільові ситуації і сповіщати про них. Є можливість налаштувати різні типи правил, такі як зміни в частоті подій, різке збільшення або зменшення кількості подій, або навіть кастомізовані правила, що використовують власні алгоритми користувача для виявлення аномалій. Це налаштовується набором правил, кожне з яких визначає запит, тип правила і набір оповіщень.

Фреймворк працює, поєднуючи Elasticsearch з двома типами компонентів, типами правил і сповіщеннями. На Elasticsearch періодично відправляється запит і дані з запиту (логи) передаються до типу правила, який визначає, чи знайдено збіг. Коли відбувається збіг, він передається одному або декільком правилам сповіщення, які вживають заходів на основі цього збігу.

Кожне правило визначає запит, який потрібно виконати, параметри, за якими спрацьовує збіг, і список сповіщень, які потрібно запустити для кожного збігу. Кожне правило являє собою окремий YAML-файл, який має містити наступні обов'язкові поля [7]:

– «es_host» і «es_port» повинні вказувати на кластер Elasticsearch, до якого ми робимо запит;

– «name»: унікальне ім'я для правила. ElastAlert не спрацює, якщо два правила мають однакову назву;

– «type»: кожне правило має свій тип, який може приймати різні параметри. Тип «frequency» означає «Сповіщати, коли відбувається більше ніж «num_events» протягом часового інтервалу»;

– «index»: назва індексу(ів) для запиту. Якщо використовується Logstash, за замовчуванням індекси будуть відповідати "logstash-*";

– «num_events»: параметр є специфічним для типу frequency і є пороговим значенням для спрацьовування оповіщення;

– «timeframe»: період часу, за який має відбутися num_events;

– «filter»: список фільтрів Elasticsearch, які використовуються для фільтрації результатів. Тут ми маємо фільтр за одним терміном для документів, у яких «деяке_поле» збігається з «деяким_значенням». Якщо фільтри не потрібні, слід вказати порожній список: filter: [];

– «alert»: список цілей, яким будуть вислані сповіщення. Сповіщення електронною поштою потребує SMTP-сервера для надсилання пошти. За замовчуванням він намагатиметься використовувати localhost. Це можна змінити за допомогою параметра smtp_host. Ще однією популярною ціллю є «telegram», для якого потрібен токен і канал;

– «email»: це список адрес, на які будуть надіслані сповіщення.

Приклад конфігурації правила зображено на рис.1.

```
name: Load average for 1 minutes over 2
type: any
index: logstash-*
num_events: 2
timeframe:
  minutes: 2
filter:
  - query:
      query_string:
        query: "system.load.1:>1"
alert:
  - "telegram"
telegram_bot_token: 6973162738:AAFyWuCEOVhu2hKlPACvj
telegram_room_id: "@elk_alert_scream"
```

Рис.1. Приклад конфігурації правила ElastAlert

У якості системи для відстеження порушень в системі було обрано OSSEC. OSSEC – це система виявлення вторгнень з відкритим вихідним кодом. Вона виконує аналіз журналів, перевірку цілісності, моніторинг реєстру Windows, виявлення руткітів, оповіщення в реальному часі та активне реагування [8]. Вона працює на більшості операційних систем, включаючи Linux, OpenBSD, FreeBSD, Mac OS X, Solaris і Windows. Вона поєднує в собі всі аспекти HIDS (Host Intrusion Detection System – виявлення вторгнень на основі хостів), моніторингу журналів та управління інцидентами безпеки (SIM)/управління інформацією та подіями безпеки (SIEM) в одному простому, потужному рішенні з відкритим вихідним кодом. Основні функції:

– перевірка цілісності файлів. Будь-яка атака супроводжується зміною системи. Мета перевірки цілісності файлів (File Integration Monitoring) – виявити ці зміни і попередити, коли вони відбудуться. Це може бути атака, зловживання з боку співробітника або навіть друкарська помилка адміністратора, про будь-яку зміну файлу, каталогу або реєстру вам буде повідомлено;

– моніторинг журналів. Кожна операційна система, додаток і пристрій у мережі створюють журнали подій, щоб повідомити вам про поточний стан системи. OSSEC збирає, аналізує та опрацьовує ці журнали, щоб повідомити вам, якщо відбувається щось підозріле (атака, зловживання, помилки тощо). Наприклад, на клієнтському комп'ютері була встановлена програма, або були внесені зміни правил у вашому брандмауері чи фаєрволі.

Обробка журналів виконується всередині OSSEC процесами logcollector і analysisd. Перший збирає події, а другий аналізує (розшифровує, фільтрує і класифікує) їх. Це робиться в режимі реального часу, тому як тільки подія записується, OSSEC обробляє її. OSSEC може читати події з внутрішніх файлів журналів, з журналу подій Windows, а також отримувати їх безпосередньо через віддалений syslog.

OSSEC постачається з набором вбудованих правил, які визначають типову активність, яку слід відстежувати в системах. За замовчуванням ці правила включають широкий спектр активностей, таких як неуспішні спроби входу, отримання доступу до важливих файлів та зміну конфігурації системи. Також користувачі можуть створювати власні правила з урахуванням специфічних вимог до їхнього середовища [9]. Приклад налаштування такого правила наведений на рис.2.

```
<rule id="5700" level="0" noalert="1">
  <decoded_as>sshd</decoded_as>
  <description>SSHD messages grouped.</description>
</rule>

  <rule id="5710" level="5">
  <if_sid>5700</if_sid>
  <pcre2>illegal user|invalid user</pcre2>
  <description>Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,</group>
</rule>
```

Рис.2. Приклад OSSEC для виявлення несанкціонованого входу до SSH

Існує головний елемент, що групує правила по типу «sshd», тобто ті, що належать до взаємодії з протоколом SSH. Поле «decoded_as» зберігає це значення, про що говорить опис «description». Дочірнє правило є більш специфічним, і реагує на конкретну подію. Воно має свій ID, дескриптор «if_sid», значенням якого є головна група. «pcre2» містить вираз, який потрібно знайти у журналах, події якого будуть відстежуватись. Одразу як таке повідомлення має збіг, OSSEC реагує моментально. Такий функціонал є дуже потужним і дозволяє створювати свої фільтри та налаштовувати критичність подій. Це допоможе більш точно виявляти серйозні інциденти.

Як було з'ясовано, наразі є велика кількість рішень, що задовольняють потреби адміністратору мережі у відстежуванні її стану, але для нашої конкретної системи основою слугуватиме ELK-стек. Для закриття недоліків ELK-стеку у вигляді відсутності механізму сповіщення і наявності правил порушення безпеки було обрано Elastalert та OSSEC HIDS через їх легке впровадження та потужний функціонал. Таким чином, проаналізувавши взаємодію серверів в мережі, необхідне ПЗ, клієнт-серверний підхід, була розроблена схема роботи майбутньої системи моніторингу, зображена на рис.3.

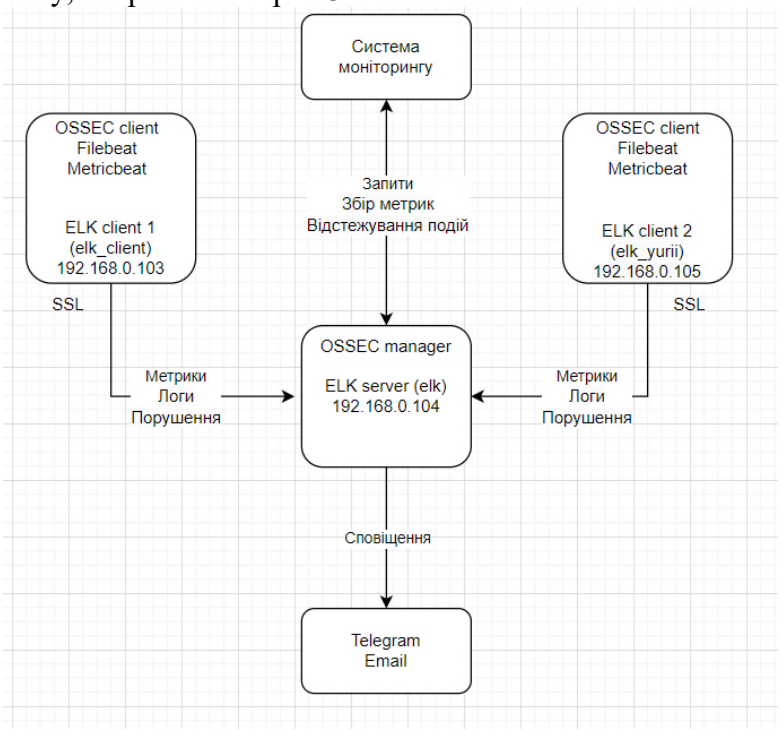


Рис.3. Схема роботи системи моніторингу в мережі

Для низького порогу входження і візуалізації у ELK-стеку бракує зручного інтерфейсу – той, що пропонує Kibana, є досить надлишковим. Тому було вирішено створити систему моніторингу, яка надавала б можливість без зайвих зусиль

відстежувати сервери, налаштовувати і додавати правила для сповіщень у популярні цільові сервіси для підвищення швидкості реакції на інциденти. Для розробки спеціалізованої системи моніторингу використовувались наступні інструменти і складові:

– мова програмування Python і модулі tkinter з Elasticsearch;
– Filebeat і Metricbeat;
– ELK-стек.

Після запуску системи моніторингу перед користувачем відкриється наступний інтерфейс, зображений на рис.4, що складається з 4 секцій:

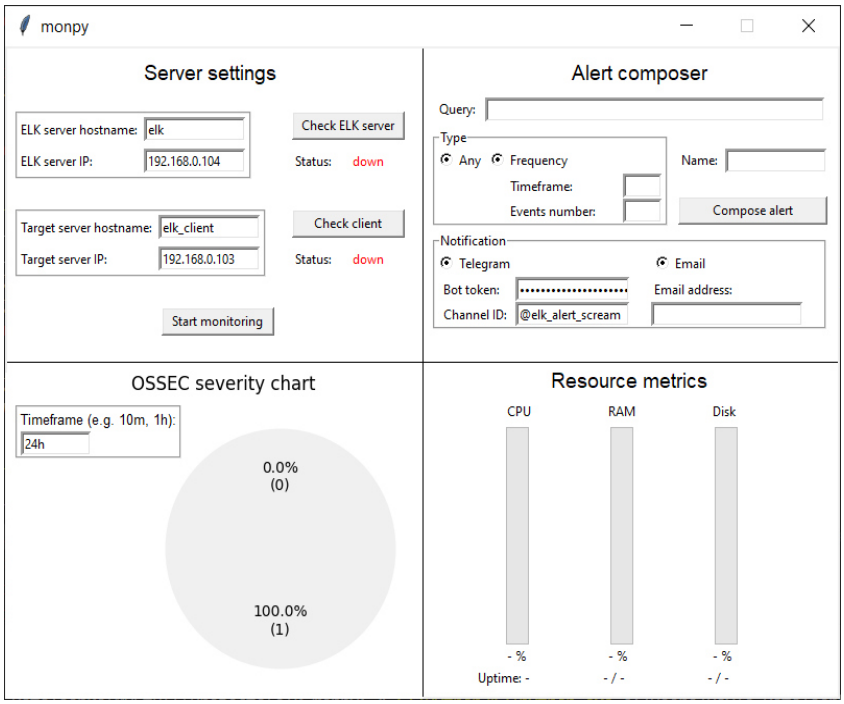


Рис.4. Початковий інтерфейс системи

Секція Server settings відповідає за внесення інформації про адресу серверу з ELK-стеком, з якого будуть збиратися події і до якого робляться усі подальші запити. Секція Resource metrics відображає поточну завантаженість цільового серверу. Додані три стовпці, які покажуть у процентному відношенні скільки ресурсів процесору було використано (стовпець CPU), об'єм оперативної пам'яті (стовпець RAM), а також зайняте місце на диску (стовпець Disk). За допомогою цих трьох показників можна досить швидко визначити стан серверу. Слідкування за ресурсами не тільки повідомить нам про необхідність розширення, наприклад, постійного накопичувача, але і повідомить про надмірну завантаженість процесору, що може свідчити про активність потенційно шкідливих процесів. Крім відображення у процентному відношенні, також надається інформація в числах, скільки усього ресурсу мається на сервері і яка кількість використовується. Для зручності додана стрічка з часом роботи машини з моменту включення (стрічка Uptime).

Секція OSSEC Severity chart являє собою діаграму критичності подій. Утиліта відслідковує і аналізує логи в системних журналах, а також стежить за процесами в цільовій системі. Кожна подія має свій «рівень небезпеки». Усього існує десять рівнів, від системного повідомлення до детектування втручання в систему, або виявлення потенційної атаки. Ранжування подій згідно з OSSEC відбувається наступним чином:

– рівні 1 - 2 вирішено опустити з причини малої цінності інформації про події, пов'язані з ними. Це можуть бути звичайні події, наприклад, перезавантаження служби операційної системи;

– низька критичність у подій рівня 3 - 4;

– середня: рівні 5 - 6;

– висока: рівні 7 - 8;

– критична: рівні 9 - 10.

В секції Alert composer ми можемо створювати файли правил сповіщень для ElastAlert. Також вона відповідає за відправлення правила на центральний сервер. На виході ми отримуємо YAML-файл, згідно нашого вводу, готовий до використання. Для створення і використання правил необхідно заповнити наступні поля:

– Query – запит, по якому будуть фільтруватись логи журналів;

– Type – панель вибору Any або Frequency. При виборі Frequency нам доступні поля Timeframe і Events number, які відповідають за проміжок часу і кількість подій, що відбулися за нього;

– Name – ім'я правила. Повинне бути унікальним для коректної роботи ElastAlert;

– Notification – панель вибору Telegram або Email. Якщо обрана позиція Telegram, необхідно надати Bot token (токен боту, що буде відправляти сповіщення) і Channel ID (ідентифікатор каналу для повідомлень). У випадку з Email, надати адресу отримувача листа зі сповіщенням.

Створимо правило для відправки сповіщення до Telegram-каналу, у якості запиту використаємо текст повідомлення про атаку перебором на SSH. Оскільки у самому правилі OSSEC вже є поля для відстеження частоти, встановимо тип Any. Введемо ім'я правила і натиснемо на кнопку Compose alert. На сервері з'явиться файл з усією відповідною конфігурацією. Приклад налаштування в секції Alert composer і результуючий YAML-файл з правилом зображено на рис.5. На рис.6 зображений приклад повідомлення на Email.

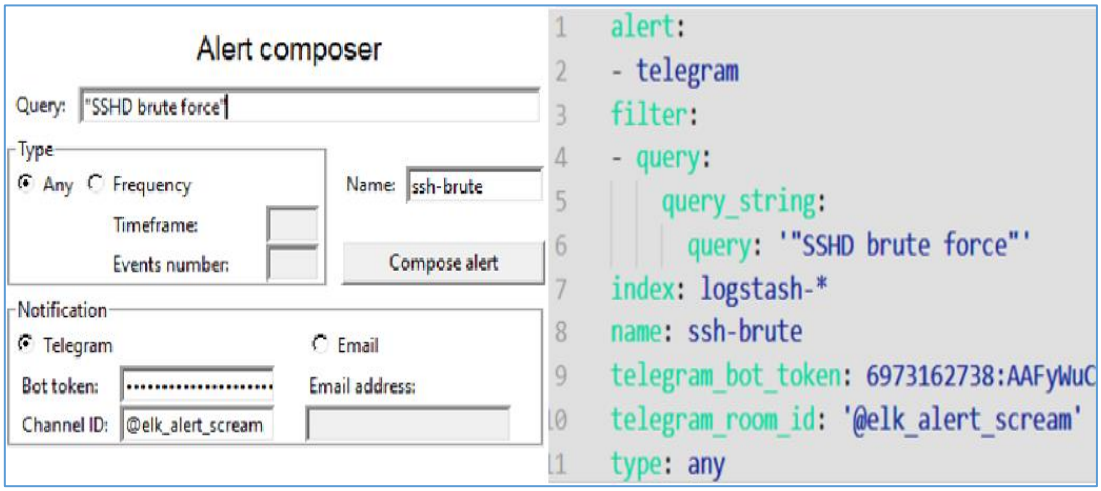


Рис.5. Налаштування Alert composer і результуючий файл з правилом

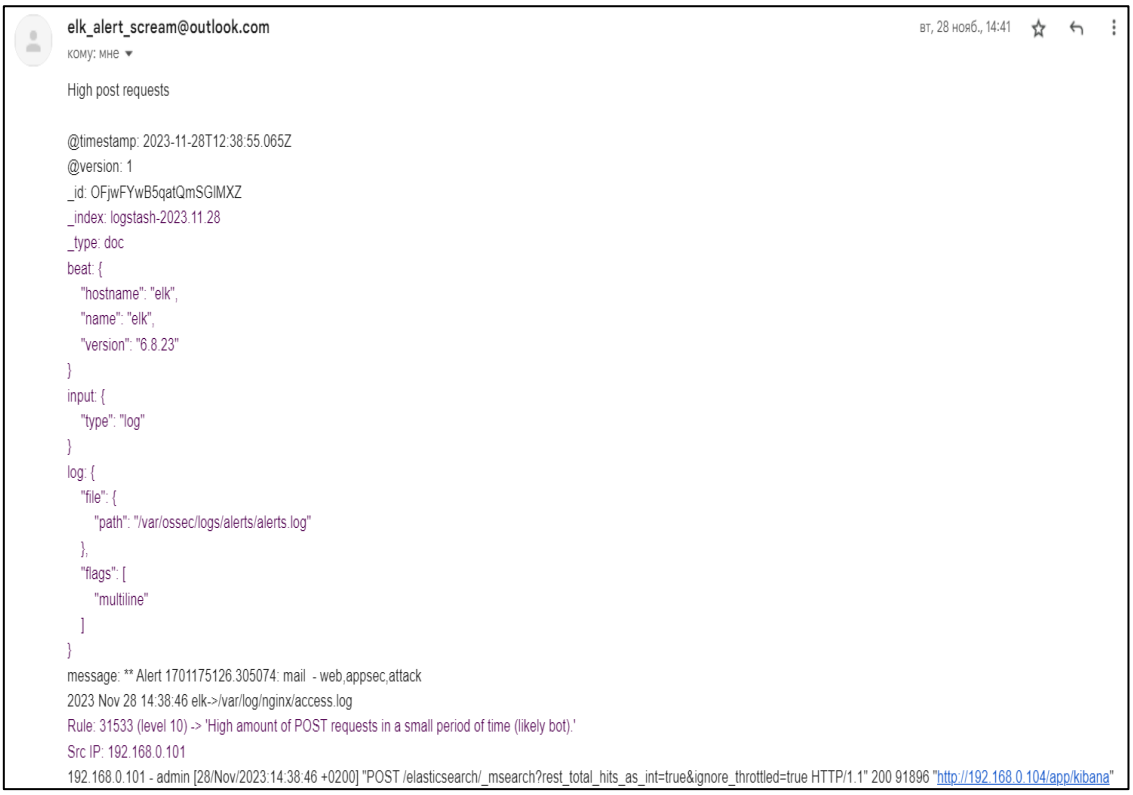


Рис.6. Приклад листа з сповіщенням на електронну пошту

На рис.7 відображена створена система моніторингу в процесі роботи, у момент відстеження доступності серверів, збору метрик і інформації про події на сервері від OSSEC. Таким чином, система дозволяє отримувати дані про стан мережі у реальному часі.

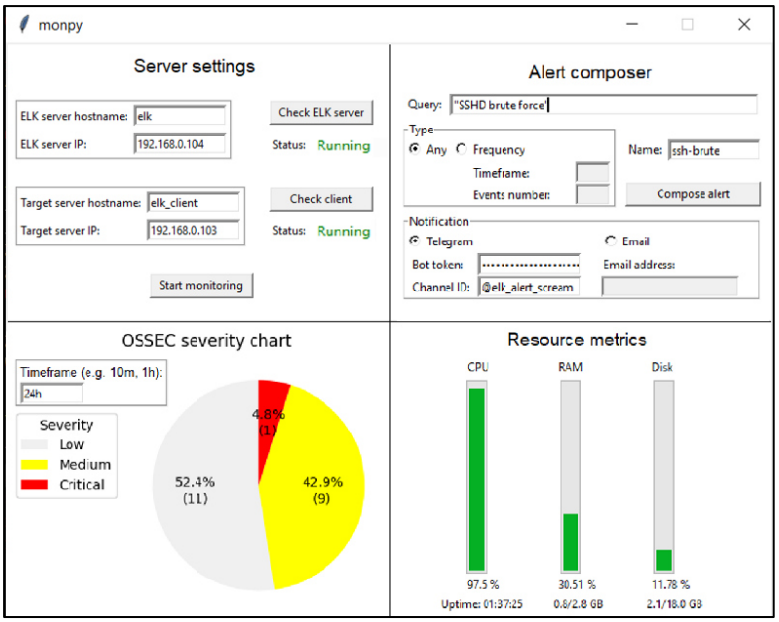


Рис.7. Система моніторингу в процесі відстежування стану мережі

Висновки. В роботі було досліджено і описано технології і способи, що використовуються для створення рішень для моніторингу, а також розроблено нову таку систему для підвищення ефективності відстежування стану безпеки комп'ютерної мережі.

Проаналізовано існуючі рішення для моніторингу мережі, здійснено аналіз таких систем, виявлено їх переваги і недоліки. У ході аналізу обраним рішенням став ELK-стек через його переваги у вартості, зручності користування, масштабованості і наявності повноцінного API.

ELK-стек не рекомендується використовувати в базовій комплектації для повноцінного моніторингу попри його потужний функціонал. Через відсутність вбудованих можливостей сповіщення адміністратора та правил кореляції ELK-стек не в змозі довершити повний набір інструментів, необхідний аналітику з безпеки. Тож він може бути доповнений іншими платформами, розширеннями і сервісами.

Наведено перелік інструментів, що були використані при розробці системи моніторингу. Покращено і доповнено функціонал ELK-стеку за допомогою побудованої на основі нього системи моніторингу. Впроваджені самостійно розроблені сповіщення з ElastAlert і правила кореляції від OSSEC для повноцінного і усебічного моніторингу стану мережі. Створено зручний інтерфейс, за допомогою якого легко і швидко можна дізнатися інформацію про стан мережі, а також створювати нові правила для сповіщень про інциденти. Подальшими кроками для покращення системи стане додавання панелей для відстежування подій безпосередньо у програмному застосунку.

Список літератури

1. Рішення Splunk. URL: https://www.splunk.com
2. LogPoint: Award winning SIEM software. URL: https://www.logpoint.com
3. Elasticsearch, Kibana, Beats & Logstash. URL: https://www.elastic.co/elastic-stack/
4. Threat Hunting Using Elastic Stack: An Evaluation. URL: https://www.researchgate.net/publication/357818741_Threat_Hunting_Using_Elastic_Stack_An_Evaluation
5. Al-Mahbashi I.Y.M., Potdar M.B., Chauhan P. Network security enhancement through effective log analysis using ELK. *International Conference on Computing Methodologies and Communicatio ICCMC.* 2017. P. 566-570. DOI:10.1109/ICCMC.2017.8282530
6. Моніторинг комп'ютерної мережі. URL: https://businessyield.com/uk/technology/network-monitoring
7. ElastAlert – Easy & Flexible Alerting With Elasticsearch. URL: https://elastalert.readthedocs.io/en/latest/elastalert.html
8. OSSEC HIDS. URL: https://www.ossec.net/docs/docs/manual/non-technical-overview.html
9. OSSEC rules composition. URL: https://www.ossec.net/docs/docs/manual/rules-decoders/create-custom.html

П.Ю. Паталашко, Н.І. Кушніренко, Н.Г. Козаченко, Н.В. Бойко

DEVELOPMENT OF INFORMATION SECURITY EVENTS MONITORING SYSTEM

P. Patalashko, N. Kushnirenko, N. Kozachenko, N. Boiko

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
e-mail: infsec2011@gmail.com

If a problem occurs on the network, IT professionals need to be sure that they will be notified and receive the necessary information to resolve it and prevent similar situations in the future. Notifications are an important element of network monitoring. When an abnormal behavior occurs on the network, the system must immediately notify IT professionals so that they can respond quickly. This is when this process becomes most effective. Network monitoring must include automatic notifications of failures and events that may affect performance. In the event of an error, such notifications should be sent via email, SMS, or other convenient channel. Dynamic networks require systems that can identify vulnerabilities in real time. Therefore, some network monitoring systems provide capabilities for collecting security data, such as network logs, application logs, and security messages. This data is collected and analyzed to detect anomalies, and in the event of threats, alerts can be sent to the appropriate IT professional. Thus, a network monitoring system allows you to: ensure a continuous workflow, monitor the status of the network and respond to possible problems in a timely manner, improve network efficiency, and increase network reliability and security. Given this, we can conclude that it is crucial to monitor networks and respond to problems in a timely manner for their successful operation. This requires the use of specialized monitoring systems that can quickly analyze the state of the network, identify problem areas, and notify the appropriate specialists. This work is focused on analyzing existing network monitoring systems, highlighting their pros and cons. The technologies and methodologies used to create such solutions were studied. A new monitoring system aimed at optimizing the process of tracking the status of network security was developed. The functionality of the system is enriched by sending notifications and implementing rules for tracking abnormal behavior in the network, which will help to better identify malicious actions and warn specialists in a timely manner.

Keywords: monitoring, ELK-stack, OSSEC, ElastAlert, incident, logs, metrics.

DOI 10.15276/imms.v13.no3-4.293
УДК 004.415.25

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 293-310

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ НАВЧАННЯ ТЕОРІЇ І ПРАКТИКИ КОМБІНАТОРНИХ ІГОР

В.М. Рувінська, А.С. Тройніна

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
emails: iolnlen@te.net.ua; anastasiyatroinina@gmail.com

Метою роботи є зменшення часу на навчання теорії і практиці комбінаторних ігор за рахунок розробки методики та системи навчання, і інтеграція її в комп'ютерну навчальну гру, що допомагає побудувати правильну стратегію гри, робить підказки для вибору оптимальних ходів, дозволяє зручно спостерігати за результатами проведених ігор, переглядати минулі ходи, робити математичні розрахунки, при цьому пропонуючи унікальний та цікавий дизайн. Як результат розроблено методику навчання та програмний продукт, що являє собою гру, яка організовує процес навчання для визначення виграшних стратегій за допомогою розробленої методики та системи навчання. Інструментами розробки є інтегроване середовище розробки Microsoft Visual Studio для програмування мовою C#; багатоплатформний інструмент для розробки дво- та тривимірних ігор Unity3d; StarUML, як інструмент моделювання бізнес-логіки застосування та використання системи управління версіями Git.

Ключові слова: методика навчання, ігровий та навчальний сценарій, навчальна програма, математична теорія комбінаторних ігор, стратегія гри, виграшна позиція, програшна позиція, XOR-сума.

Вступ. Гра може стати чудовим засобом формування освітнього, розвиваючого та інтелектуального потенціалу особистості. Давно ігри стали використовувати під час навчання іноземних мов, правил дорожнього руху, програмування, популярні розвиваючі ігри для дітей та інші.

Створення навчальних комп'ютерних ігор є одне із важливих напрямів у комп'ютеризації навчання. Поєднання емоційної привабливості, яке притаманне грі, та аудіовізуальних, обчислювальних, інформаційних та інших можливостей обчислювальної техніки несе у собі великий дидактичний потенціал, який може і має бути реалізований у навчальній практиці. Особливо ефективне застосування таких навчальних ігор у областях, де потрібно придбання та розвиток навичок [1]. Крім них, існує ціла низка ігор, які використовуються при вивченні нового матеріалу, закріпленні пройденого. За своєю дидактичною спрямованістю найбільш поширеними та дієвими виявилися ігри, призначені для контролю оцінки знань та умінь учнів [2].

Навчальна гра може розглядатися як навчальна система, в якій процес навчання інтегрований в гру. Якісні навчальні ігри зберігають можливість навчальних систем і, в той же час, володіють великим мотиваційним потенціалом. Ключовою характеристикою якості навчальної гри є баланс ігрової і навчальної компоненти, що забезпечує цілісність сприйняття гри і можливість досягнення цілей навчання.

В роботі обрана предметна область, що стосується комбінаторних ігор, в зв’язку з тим, що їх теорія достатньо складна для навчання, з одного боку, а, з другого, існують такі ігри, і щоб в них грати, треба знати теорію, з третього, в них цікаво грати. Отже пропонується створення систем для навчання теорії і практиці простих комбінаторних ігор. що дозволяють грати в комбінаторні ігри, а також

допомагають побудувати правильну стратегію гри, зберігаючи при цьому ігрову привабливість.

Виходячи з вищесказаного, можна стверджувати, що впровадження навчальних ігор в освітній процес є однією з найважливіших задач. Проблема, що лягла в основу дослідження, полягає в тому, що існуючі рішення по інтеграції навчального процесу в ігровий контекст, як правило, обмежені можливістю застосування в одному програмному продукті і не можуть бути перенесені на розробку нових. Рішення полягає в розробці узагальнюючої методики навчання для схожих задач і інтеграцію її в різні навчальні системи, що і реалізовано на прикладі простих комбінаторних ігор.

Загальні відомості про комбінаторні ігри. Комбінаторні ігри – це ігри двох гравців з повною інформацією і без випадкових та прихованих ходів з виграшним або програшним результатом. Випадкові ходи притаманні, наприклад, іграм в карти, а приховані - таким іграм, як «морський бій" і "камінь-ножиці-папір". Таким чином, комбінаторна гра визначається множиною позицій, включаючи початкову позицію, і гравцем, чия черга робити хід. Гра змінюється від однієї позиції до іншої, гравці роблять хід по черзі до тих пір, поки не досягнута кінцева позиція. Кінцева позиція - це позиція, в якій немає можливих ходів. Досягнувши кінцевої позиції один з гравців оголошується переможцем, а другий тим, хто програв. Розглядають рівноправні ігри, правила яких не роблять різниці між гравцями; нерівноправні ігри, в яких кожен гравець в заданій позиції має різні набори можливих ходів (такі ігри, як шахи або шашки, в яких один гравець грає білими фігурами, а другий чорними, є нерівноправними).

Критичний огляд існуючих навчальних комбінаторних комп'ютерних ігор та засобів навчання. Перш за все існують програмні системи для найбільш популярних комбінаторних ігор. В Lucas Chess [3] та Arena [4] наявний шаховий наставник, що слідкує за ходами користувача та робить підказки, тобто гравець може задати певну позицію, а програми аналізують партії та надають найкращі для користувача варіанти розвитку. У Lucas Chess включені десятки тисяч підготовлених позицій, таких як різні види ендшпілю, тактичних комбінацій і шахових проблем, починаючи від мату в 2, 3, 4 і більше ходів, реалізується експорт/імпорт шахових партій. Навчальний процес містить широкий вибір вправ для підняття свого рівня гри: задачі на пошук мату, знайти кращій хід, задача дня, навчання з книгою, вивчення тактик методом повторення, вивчення дебютів методом повторення та інші. Arena - це клієнтська програма, що дозволяє підключити будь-який шаховий движок, який підтримує протоколи UCI чи Winboard. має невелику вбудовану дебютну бібліотеку з різноманітними партіями, а також може зберігати шахові партії.

Aurora Borealis [5] – шашкова програма, що об'єднує в собі можливості гри і роботи з шашковими базами партій, присутня можливість завантажувати навчальну літературу в певному форматі. При відображенні ігрової ситуації користувач може отримати довідкову інформацію по цій позиції. Також користувач може встановити в програмі будь-яку позицію, а Aurora підкаже найкращий варіант гри в ній: в яких партіях вона зустрічалася, як далі розвивалися події, а також, про те, як розігрування цієї позиції трактується шашковими підручниками Пропонується проста методика самонавчання.

SmartGo [6] надає можливість користувачеві зіграти партію в Go, а також навчатися цій грі. Бібліотека програми нараховує більш ніж 94000 професійних партій, орієнтуватись по яким допомагають функції пошуку та фільтрації. SmartGo в змозі серед усіх партій знайти необхідні позиції та показати статистику того, як часто даний хід обирався професіоналами. Можна порівняти свою гру з

партіями професіоналів. Також програма включає більше 2000 задач різних рівнів складності і є можливість створення свого набору задач.

Wzebra [7] – програма для гри у реверсі. Гра ведеться на заданій користувачем складності: від новачка до професіонала. Програма підтримує ряд корисних у навчанні функцій: відображення можливих ходів, повернення ходу в разі помилки, автоматичні ходи. Для максимально кращого результату WZebra може розрахувати варіанти ходу для позиції, заданої користувачем. Навчання може проводитись через спеціальний режим гри з кількісною оцінкою всіх можливих в даній позиції ходів.

Існує ряд систем, які реалізують математичну гру “НІМ”, але не навчають, як грати оптимально. А програм, з якими можна пограти в “НІМ з обмеженнями” та “Дати” не існує зовсім.

Порівняння систем було проведено переважно за характеристиками, які впливають на процес навчання та реалізовані у розробленій навчальній грі. Здебільшого подібні системи не містять теоретичних матеріалів, навчання не має певного сценарію, а ведеться під час самої гри за рахунок системи підказок та аналізу позицій. Саме тому є актуальною розробка навчальної системи, в якій були б реалізовані вищеперераховані засоби навчання та контролю знань, а також вищезазначені комбінаторні ігри “НІМ”, “НІМ з обмеженнями” та “Дати”.

Постановка задачі. Метою дослідження є зменшення часу на освоєння математичної теорії комбінаторних ігор і збереження ігрової привабливості на базі створеної методики навчання теорії комбінаторних ігор за допомогою інтерактивних комп’ютерних систем.

Для досягнення мети вирішуються наступні задачі:

– проаналізувати існуючі класи навчальних комп'ютерних ігор для віднесення комбінаторних ігор до класу(ів);

– проаналізувати підходи до інтеграції процесу навчання в комбінаторні ігри та вибрати необхідний(і);

– вибрати тип сценарію(їв) для комбінаторних ігор;

– провести систематизацію учбового курсу про комбінаторні ігри та розробити навчальні сценарії з елементами гри;

– розробити узагальнену методику для навчання комбінаторним іграм;

– реалізувати створену методику у комп'ютерних комбінаторних іграх.

Розроблена програмна система повинна мати наступні функціональні можливості:

– гра з точно відтвореними правилами настільної гри «НІМ», «НІМ з обмеженнями» та «Дати»;

– навчальна гра, що вирішує задачу навчання теорії виграшної стратегії;

– аналіз та отримання підказок по позиції;

– інструмент для математичних розрахунків у двійковій системі;

– перегляд попередніх ходів та аналіз ходів комп’ютера;

– тренувальний режим рандомних позицій за певний час з записом статистики у файл (кількість правильних та неправильних відповідей; кількість розв’язаних позицій за певний час; час який пішов на вирішення одної позиції тощо);

– перегляд теоретичних матеріалів.

Опис ігор “НІМ”, “НІМ з обмеженнями”, “Дати”. Розглянемо далі конкретні прості комбінаторні ігри, на яких випробувана запропонована методика [8].

НІМ. Два гравці по черзі беруть предмети з купок. Позиція гри може містити довільне число купок та предметів, а також формується вона до початку гри. За один хід гравець може взяти будь-яку кількість предметів з будь-якої купки: навіть

всю купку повністю, але хоча б один предмет необхідно взяти, і брати предмети потрібно з однієї купки. Гравець, що взяв останній предмет – перемагає.

Позиція в НІМ записується шляхом перерахування розмірів наявних купок, наприклад, (n_1, n_2, n_3) – позиція, в якій є три купки, в першій n_1 предметів, в другій n_2 предметів, а в третій – n_3.

Позиція, в якій хід належить гравцеві, що зможе довести партію до виграшу, ведучи правильну гру, називається виграшною. Будь-яка інша позиція називається програшною. Який би хід гравець в програшній позиції не зробив, його противник зможе виграти, якщо буде робити оптимальні ходи. Оптимальний (найкращий) хід у виграшній позиції полягає в тому, що гравець повинен залишити своєму противнику програшну позицію.

Гравець має виграшну стратегію тоді і тільки тоді, коли XOR-сума розмірів купок відмінна від нуля. В іншому випадку поточний гравець знаходиться в програшному стані. Опинившись в стані з нульовою XOR-сумою, гравець не зможе вийти з цього стану – при будь-якому його переході в стан з ненульовою XOR-сумою у противника знайдеться відповідний хід, який повертає XOR-суму назад в нуль.

Для того, щоб гравець при правильній грі доводив партію до перемоги, пропонується наступна стратегія (при виконанні ходу з певної позиції):

Приклад позиції: (2, 3, 6) 010 011 110

1. Знаходимо XOR-суму розміру купок (S) S = XOR (010, 011, 110) = 111

2. Якщо вона ненульова, то це виграшна позиція, інакше – програшна. Якщо позиція програшна, та якщо інший гравець буде грати оптимально, то виграє інший гравець. Якщо позиція виграшна, треба зробити оптимальний хід (п. 3-5).

S = 111 <> 0 – виграшна позиція

3. Знаходимо в цій сумі S в двійковому коді місце першої зліва (старшої) одиниці.

В сумі S є одиниця в старшій позиції.

4. Знаходимо купку, в якій є одиниця в цій же позиції (така хоча б одна купка є, інакше б і в XOR-сумі не було б одиниці).

Це третя купка, де 6 предметів.

5. Знаходимо XOR-суму S і розміру знайденої купки – отримуємо кількість предметів, яке потрібно залишити в знайденій купці при оптимальному ході.

XOR (111, 110) = 001

В третій купці треба залишити один предмет, тобто, забрати – 5. Це і буде оптимальний хід.

НІМ з обмеженнями. У грі НІМ за один хід можна було брати будь-яку ненульову кількість предметів з однієї купки. В НІМ з обмеженнями за один хід можна брати не будь-яку кількість предметів, а, тільки одну або декілька наперед заданих кількостей, наприклад, 3 або 5. Гра змінилась незначно, проте рішення, що було застосоване до класичного НІМ, вже не працює.

Спочатку розглянемо спрощену гру, коли є тільки одна купка з деякою кількістю предметів. Треба, аналогічно НІМ, вміти узнавати, програшна це або виграшна позиція в залежності від кількості предметів. І, аналогічно НІМ, гравець при оптимальній грі буде переводити суперника в програшну позицію. Виграшність позиції визначається за допомогою чисел Гранді для позиції. Якщо число Гранді дорівнює 0, то це програшна позиція, інакше - виграшна. Використовується для розрахунку чисел Гранді допоміжна функція mex від множини чисел, яка повертає найменше невід'ємне число, що не зустрічається в цій множині.

Також будується орієнтований граф гри, вершинами якого є позиції, а ребра позначають можливі переходи між позиціями. Розрахунок чисел Гранді

починається з вершин без вихідних ребер, з яких не можна перейти нікуди — це кінцеві програшні позиції, в них числа Гранді дорівнюють 0. Теорема Гранді говорить, що для того, щоб знайти число Гранді для позиції (вершини) V, треба знайти значення функції mex від множини вершин, в які є перехід з V. Таким чином, можна рекурсивне розраховувати числа Гранді для всіх вершин, починаючи з тих, що не мають виходів.

Знаючи числа Гранді для кожної вершини, можна оптимально грати в гру НІМ з обмеженнями з однією купкою. Часто буває, що в числах Гранді є закономірності, зокрема, періоди, і це можна використовувати для спрощення розрахунків.

Тепер, якщо купка не одна, а декілька, то така гра розглядається як сума ігор для всіх купок, і число Гранді для такої гри розраховується як XOR-сумі чисел Гранді для кожної з ігор-доданків.

Ретроспективний аналіз. Існують різні способи вирішення задач з іграми. В загальному випадку можна використовувати так званий ретроспективний аналіз [9]. Для оптимальної гри, аналогічно НІМ з обмеженнями, необхідно завчасно тим чи іншим способом для кожної позиції розрахувати, виграшні вони чи програшні, зокрема, за допомогою проходу від кінцевих позицій до всіх останніх. А далі можна кожного разу переводити суперника в програшну позицію. Так вирішується, наприклад, гра «Дати». На вході задаються дві дати: початкова і заключна. Гра починається з першої більш ранньої дати Кожен гравець на своєму ході називає пізнішу дату, збільшуючи на 1 або 2 або день у місяці, або місяць, але не те й інше відразу. При цьому поєднання дня та місяця має залишатися датою. Гравець, який назвав останню дату, програє. Використовується ретроспективний аналіз, коли до початку гри заздалегідь розраховується для кожної дати (дня) року на діапазоні початкова дата - заключна дата, виграшна вона, чи програшна, якщо обидва гравця будуть грати оптимально. Рухаючись у зворотному напрямку, починаючи з заключної, переходять до позицій, які переводяться в заключну за 1 хід, потім – до позицій, які переводяться в заключну за 2 ходи, і так далі, поки не буде досягнута початкова позиція.

Класифікація навчальних комп'ютерних ігор. Навчальна комп'ютерна гра – це форма навчально-виховної діяльності, що імітує ті чи інші практичні ситуації, є одним із засобів активізації навчального процесу, сприяє розумовому розвитку. По суті навчальна комп'ютерна гра є дидактичною грою, організованої на більш високому технічному рівні. Розроблено та успішно використовуються в навчальному процесі електронні навчальні курси і системи, досліджуються і аналізуються методи і результати їх застосування [10-12]. Вчені постійно розробляють і пропонують до впровадження нові, більш досконалі методи, що дозволяють істотно підвищити якість і інтенсифікувати процес навчання. Для вибору правильного підходу для навчання теорії і навичкам комбінаторних ігор необхідно знати види комп'ютерних навчальних ігор і вплив кожної з них на людину. Аналізуючи програмне забезпечення, можна сказати, що комп'ютерні ігри мають великі можливості для загального інтелектуального і емоційно-особистісного розвитку людей і їх навчання. Розглянемо далі класифікації комп’ютерних ігор за різними критеріями. За цілями і завданням навчальні комп'ютерні програми діляться на: які ілюструють, що консультують, програми-тренажери, програми навчального контролю, операційні середовища. Ігри можна ділити на підгрупи, виходячи з різних критеріїв: вікового, сюжетної тематики, рівня складності ігрових завдань, складності управління, завдань розвитку розумових здібностей та інших характеристик. У великому асортименті освітніх ігор виділяється велика група навчальних і розвиваючих комп'ютерних ігор, які спеціально створюються для використання в освітніх цілях. Це і окремі програми,

і набори програм, які представлені у вигляді окремих колекцій, пакетів, серій – залежно від ступеня їх «спільності». Але, в першу чергу, всі освітні ігри можна згрупувати в такі великі класи: розвиваючі ігри, навчальні ігри, ігри-експериментування, діагностичні ігри, ігри-забави, тренувальні і комбіновані. Для нашого дослідження необхідно, з одного боку, розглянути систематизацію комп'ютерних ігор взагалі, а, з другого, зокрема, класифікацію навчальних комп'ютерних ігор. Класифікація ігор потрібна не тільки для зручності гравця, але й педагогам стає легше орієнтуватися у всьому багатстві ігор, і розробникам дозволяє визначитись, яких ігор недостає для формування тієї чи іншої компетентності. На рисунку 1 представлена класифікація комп'ютерних ігор, що включає дев'ять категорій [13].

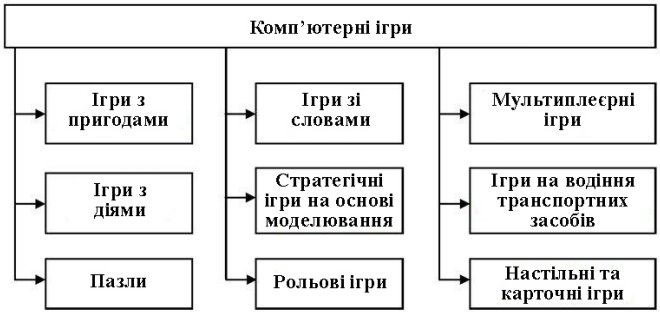


Рис. 1. Класифікація комп'ютерних ігор

При класифікації комп'ютерних ігор, призначених для навчання, використовують деревоподібну структуру, що включає кілька рівнів:

1-ий рівень – вік, на який направлена гра (наприклад, діти 5-6 років, школярі 7-го класу, студенти, дорослі). Наша аудиторія – школярі старших класів, студенти та дорослі.

2-ий рівень – навчальна дисципліна, для вивчення якої призначена гра. Це може бути дисципліна "Теорія ігор" або "Комбінаторна теорія ігор".

3-й рівень – тема навчальної дисципліни. Тема: "Оптимальні стратегії для ігор НІМ, НІМ з обмеженнями, Дати".

4-й рівень – вибір класу, тобто, який тип гри підходить для рівнів 1-3. З класифікації ігор, що представлена на рисунку. 1, нам цікава категорія настільних ігор, адже комп'ютерні комбінаторні ігри зародились на основі настільних логічних ігор.

5-ий рівень - який з методів класичного навчання може підтримувати гра. Такі методи, що надають можливість набуття нових знань, тренінгу та напрацювання досвіду вирішення математичних задач, які притаманні комбінаторним іграм, та перевірки знань та умінь.

Аналіз підходів до інтеграції процесу навчання в гру. Підхід до інтеграції процесу навчання в гру залежить від внутрішнього уявлення (моделі) предметної області, що вивчається в грі. За способом подання предметної області можна виділити ігри на основі імітаційного моделювання, на основі ситуаційного моделювання і на основі формально-логічної моделі [14].

Імітаційні моделі реалізується в іграх-симуляторах (simulator), які моделюють реальні умови професійної діяльності фахівця в деякій галузі знань. До цього класу ігор відносяться симулятори управління різними транспортними засобами, медичні, тактичні, соціальні та бізнес-симулятори. Розробка симуляторів включає розробку реалістичної моделі процесу у відповідній предметній області, що складає предмет вивчення в грі [15, 16]. Наприклад, розробка авіа-симулятора (Microsoft® Flight Simulator X, X-Plane та ін.) вимагає створення моделей фізичної складової (симуляція параметрів літака і його взаємодії з середовищем) і моделей графічної складової (віртуальна чи реальна

машина пілота). Ігрова складова в таких іграх реалізується з використанням багатих графічних і звукових можливостей сучасних засобів обчислювальної техніки для комп'ютерної інтерпретації реальних процесів.

Формально-логічні моделі предметної області використовується у таких іграх, як пазли (puzzle games), ігри на зіставлення об'єктів (matching games), різні варіанти ігор на тренування пам'яті (memory games, brain training games) Такі ігри ґрунтуються на перевірці відповідності даних, що вводяться гравцем, заданим в системі патернам. Введені дані інтерпретуються як висловлювання на певній мові, заданою граматикою, формально-логічна модель використовується для перевірки істинності висловлювань.

Ситуаційні моделі використовуються в іграх, де реалізовано навчання на прикладах (“case study”-підхід) [17] з використанням можливостей комп'ютерних ігор (організація діалогів, візуалізація персонажів, подій і місця існування тощо). Ці ігри, як правило, реалізуються в рольовому (role-playing) або пригодницькому (adventure) жанрі. Гравець поміщається в віртуальне середовище, створене на основі описів ситуацій з реальної дійсності, діє відповідно до закладеного в гру сценарію (планом дій), веде попередньо передбачені в грі діалоги, вибирає свої рішення з заданих наборів і в результаті навчається на прикладах правильних рішень. Процес проектування таких ігор включає розробку опису, ігрового сюжету на основі сценарію, розробку віртуального середовища і способу її відображення. Основним завданням розробників таких навчальних ігор є вибір і реалізація способів найбільш привабливого з ігрової точки зору відтворення сценарію.

Комбінаторним іграм найбільше підходить за концепцією *ситуаційна* модель, саме так у роботі запропоновано навчання: гравець поміщається в віртуальне середовище, діє відповідно до сценарію, веде діалоги, приймає рішення, їх система перевіряє на правильність і, в результаті, навчається на своєму досвіді.

Навчальні сценарії з елементами гри. Спосіб інтеграції процесу навчання з ігровим процесом визначається способом взаємодії в грі ігрових і навчальних дій, тобто способом інтеграції навчального курсу в ігровий сценарій. Під сценарієм навчальної гри розуміють набір взаємопов'язаних елементів сценарію, що представляють ігрову і навчальну компоненти.

В основу навчального сценарію, що визначає зміст предметної області, яка оперує абстрактними поняттями, в тому чи іншому вигляді покладені деякі базові об'єднуючі принципи, на яких будується весь зміст. Інтерпретація таких предметних областей в ігровому контексті може бути реалізована в штучно створеному віртуальному ігровому світі, в якому ключові поняття предметної області інтерпретуються як система правил, аксіом, сутностей, відносин віртуального світу. Навчальні завдання, необхідні для розвитку навичок в досліджуваної предметної області, інтерпретуються як проблеми ігрового світу, відповідно рішення завдань є рішеннями ігрових проблем.

Таким чином, кожен елемент предметної області інтерпретується як елемент ігрового сценарію. Предметною областю для нас слугує комбінаторні ігри: відповідно ігровий сценарій, сама гра та функціонал, який покладено у гру. При цьому множина елементів може доповнюватися елементами сценарію, які не є інтерпретаціями предметної області, таким чином, що при цьому не порушуються логічні зв'язки між елементами, що визначають навчальний сценарій. Алгоритм, який визначає виграшну стратегію – це навчальний сценарій. Він формує знання щодо вирішення проблем, які стоять у предметній області шляхом візуалізації понять «завдання-рішення-оцінка».

Під сценарієм навчальної гри розуміють *набір* взаємопов'язаних елементів, що представляють *ігрову і навчальну компоненти.* Домінування в грі навчальної

або ігрової компоненти визначає тип сценарію, реалізованого в грі. Виділяють чотири способи організації сценаріїв в навчальних іграх [14]: навчальний сценарій; навчальний сценарій з елементами гри; незалежні ігровий і навчальний сценарії; ігровий сценарій з елементами навчання. Але найбільш ефективним є так званий *комбінований сценарій*, коли *ігрові та навчальні завдання виконуються одночасно*, що дозволяє забезпечити баланс ігрової і навчальної компоненти. «У цьому випадку гравець буде прагнути досягти ігрової мети, але при цьому він неявно буде прагнути до досягнення мети навчання, тобто ігрова мета буде досягатися як мета навчання» [11]. Саме такий комбінований сценарій пропонується для навчальних комбінаторних ігор у зв'язку зі складністю вивчення цього матеріалу, і це дозволить гравцю легше пройти навчання, майже не помітивши його (не акцентуючи увагу) в процесі гри.

Сценарій навчання будується на основі алгоритму виграшної стратегії і вбудовується в ігровий процес. Усі рішення гравця у навчальному сценарії обробляються, в разі невірних пропонуються вірні або повернення на потрібну кількість кроків назад, і в результаті гравець навчається виявляти виграшні стратегію для комбінаторної гри. Для кожної з ігор "НІМ", «НІМ з обмеженнями», «Дати», стратегія різна, відповідно і навчальний сценарій різний, але ці стратегії мають спільні риси, тому що ці ігри одного класу – комбінаторні.

Методика навчання комбінаторним іграм на прикладі ігор НІМ, НІМ з обмеженнями і Дати. Систематизація навчального курсу**.** Для кращого засвоєння навчального курсу його необхідно систематизувати та поділити на певні етапи. У табл. 1 представлена систематизація навчального курсу з комбінаторної теорії ігор в ігровому контексті у вигляді пунктів навчання, які повинен пройти користувач для отримання знань.

Таблиця 1

Систематизація навчального курсу в ігровому контексті

Розділ курсу навчання		Реалізація
Теоретичні відомості		Користувач отримує інформацію, щодо теорії комбінаторних ігор.
Ретроспективний аналіз	Аналіз	Користувач отримує інформацію, щодо теорії ретроспективного аналізу комбінаторних ігор.
	Ігри на графах	Користувач отримує інформацію, щодо теорії графів, побудови орієнтованих графі, їх використанню при ретроспективному аналізі комбінаторних ігор.
	Опис алгоритму	Користувач отримує інформацію про алгоритм ретроспективного аналізу .
НІМ	Попередня підготовка	Будується граф з позиціями гри та можливими переходами між ними. Для кінцевих позицій, а також декількох тих, що їм передують, визначається їх виграшність або програшність для кожного з гравців.
	Алгоритм виграшної стратегії гри	Користувач навчається виграшній стратегії, що складається з двох етапів: визначення виграшності стану гри за допомогою XOR та оптимального ходу.
НІМ з обмеженнями	Теорія Шпрага-Гранді	Користувач отримує інформацію про теорію Шпрага-Гранді, яка визначає оптимальну гру у «НІМ з обмеженнями».
	Попередня підготовка	Будується граф з позиціями гри та можливими переходами між ними. Для всіх позицій, починаючи з кінцевих, а також декількох тих, що їм передують, визначається їх виграшність або програшність для кожного з гравців.

продовження таблиці 1

	Алгоритм виграшної стратегії для ігор з однією купкою	Користувач навчається виграшній стратегії, що складається з двох етапів: визначення виграшності стану гри на основі чисел Гранді та оптимального ходу.
	Алгоритм виграшної стратегії для ігор з декількома купками	Користувач навчається виграшній стратегії, що складається з двох етапів: визначення виграшності стану гри на основі концепції суми ігор та оптимального ходу.
Дати	Попередня підготовка	1) Будується граф з позиціями гри та можливими переходами між ними. Для кінцевих позицій, а також декількох тих, що їм передують, визначається їх виграшність або програшність для кожного з гравців. 2) Для кожного можливого стану гри визначається заздалегідь його виграшність або програшність на основі станів, для яких вже визначено виграшність.
	Алгоритм виграшної стратегії	Користувач навчається виграшній стратегії, що складається з двох етапів: визначення виграшності стану, що вже стало відомо при попередній підготовці, та оптимального ходу.

Сценарій для гри НІМ. Так як метою дослідження є зменшення часу на освоєння математичної теорії комбінаторних ігор і збереження ігрової привабливості, то проектування та розробка методики на основі ситуаційної моделі навчального сценарію з елементами гри буде найбільш ефективною. У табл. 2 наведені елементи ігрового сценарію, що об'єднує навчальні та ігрові дії, і реалізує таким чином модель навчального сценарію з елементами гри для «НІМ».

Таблиця 2

Опис елементів ігрового та навчального сценарію гри «НІМ»

Сценарій	Зміст елемента	
Навчальний	"Ти вже знаєш, що таке НІМ і як у нього грати. Давай тепер розглянемо певну гру."	
Ігровий	Виводимо предмети на екран у три купки, кількості 3, 2 та 1. Натискаємо “Далі”.	
Навчальний	"Для того, щоб розібратися з цим, давайте розглянемо різні ігрові позиції. По-перше, скільки в цій грі ігрових позицій?"	
Навчальний	" Перерахуємо все (у фігурних дужках ми писатимемо число каменів у купках): {1}, {2}, {3}, {1,1}, {2,1}, {3,1}, {2,2}, {3, 2}, {1,1,1}, {2,1,1}, {3,1,1}, {2,2,1}, {3,2,1}."	
Навчальний	"Це позиції, в які ми можемо потрапити через кілька ходів. Розмістимо дані позиції на графі."	
Ігровий	Виводимо граф із усіма позиціями. Перегляд графа.	
Навчальний	"Очевидно, що починаючи з позиції {1,1} виграє другий гравець, а з позицій {1}, {1,1,1} виграє перший. Спробуй далі сам визначити виграшність позицій."	
Ігровий	Позначаємо на графі виграшність цих позицій. Виводимо поля для введення виграшності інших позицій. Перевіряємо дані, що введені гравцем.	
Навчальний	"Відповідно можна визначити виграшну стратегію – до яких вершин потрібно переходити, щоб виграти." "Але будувати для кожної гри під час попередньої підготовки її повний граф довго, а іноді й складно. Давай тепер розглянемо як інакше визначити виграшну стратегію."	
Ігровий	Виводимо любу гру. Тут початковий стан може бути чи виграшний, чи програшний, тому далі показані обидва варіанти.	
Навчальний	"Ця позиція виграшна!"	"Позиція програшна. Тут можна ходити по-різному, на твій вибір."
Ігровий	Кнопки: "Чому?". Натискання.	

продовження таблиці 2

Навчальний ("Чому?")	"XOR-сума кількостей предметів у купках ненульова. Отже можна перевести цю позицію в нульову, щоб залишити супротивника в програшної позиції."	"Оскільки XOR-сума нульова. Значить сходити в нульову позицію, щоб залишити супротивника в програшній, не вдасться. Ходи."
Ігровий	Кнопки: "Як виграти?"	
Навчальний	"Знаходимо XOR-суму кількостей для всіх купок. Назвемо її S." "Порахуй суму: … Введи у поле: <поле>"	
Ігровий	Вивід поля для вводу числа. Введення чисел.	
Навчальний	"Правильно."	"Невірно. Вважай уважніше або подивися як вважається XOR-сума. Правильна відповідь: (res)."
Навчальний	"Тепер знаходимо в цій сумі, в двійковому коді, місце першої одиниці. Знаходимо купку, в якій є одиниця в цій же позиції. Така хоча б одна купка є, інакше б і в XOR-сумі не було б одиниці." "Це (номер - x) купка - (двійкове уявлення)."	
Навчальний	"Порахуй XOR-суму S і розміру знайденої купки – отримуємо кількість предметів, яке потрібно залишити в знайденій купці при оптимальному ході." "Введи в поле:<поле>"	
Ігровий	Вивід поля для вводу числа	
Навчальний	"Так"	"Невірно. Вважай уважніше або подивися як вважається XOR-сума." "Відповідь: (res)"
Навчальний	"Значить нам потрібно залишити в купці (x) рибок, тобто забрати необхідно інші."	
Ігровий	Користувач робить хід у грі.	
Навчальний	"Чудово! Все правильно."	"Ти впевнений, що хочеш так бути схожим? Це може призвести до програшу!"
Навчальний	"Тепер ти знаєш, як грати в НІМ, використовуючи виграшну стратегію." "Спробуй далі визначити сам, скільки каменів і звідки потрібно брати. Для цього тобі знадобиться блокнот для розрахунків."	
Ігровий	Користувач може робити ходи. Навчальна система слідкує за ним та, якщо він ходить невірно, поправляє його.	

Сценарій для гри НІМ з обмеженнями. Обмеження — це можливість взяти з купки не довільну кількість предметів, а обмежену. Спочатку будемо розглядати спрощену гру з однією купкою.

У табл. 3 наведені елементи ігрового сценарію, що об'єднує навчальні та ігрові дії, і реалізує таким чином модель навчального сценарію з елементами гри для «НІМ з обмеженнями з однією купкою».

Таблиця 3

Опис елементів сценарію гри «НІМ з обмеженнями з однією купкою»

Сценарій	Зміст елемента
Навчальний	"Отже, ти вже знаєш, що в НІМ з обмеженнями ми можемо брати лише обмежену кількість каменів, наприклад, 2 і 3. На перший погляд гра змінилася незначною, але це не так. Те рішення, яке ми розглядали для класичного НІМ-у, Для цього нам потрібно розглянути теорію Шпрага-Гранді, яка складається з 4 частин, і освоєння кожної поступово наближає нас до вирішення завдання.
Ігровий	Вікна: «1. Спрощений варіант гри: одна невелика купка, ретроспективний аналіз», «2. Функция mex», «3. Числа Гранди», «4. Закономірності в числах Гранди». В кожному з пунктів виводиться теоретичний матеріал.
Ігровий	Перегляд вікна 1. Спрощений варіант: одна невелика купка, ретроспективний аналіз.

продовження таблиці 3

Навчальний	"Розглянемо спочатку спрощену гру з однією купкою: є одна купка, в ній 6 предметів, кожен гравець може взяти, припустимо, лише 2 або 3 предмети. Програє той, хто нічого не може взяти." "Таким чином, якщо залишилося 0 або 1 предмет, то нічого не можна взяти - і це програшна ситуація. Тому розглядатимемо стани гри, починаючи зі станів, з яких вже нікуди не можна піти (0 і 1). Визначимо виграшність наступних станів, використовуючи ретроспективний аналіз"
Ігровий	Виводимо граф зі станами гри - 6 позицій (тому що у нас 6 предметів).
Навчальний	"З позиції 2 можна перейти в позицію 0. Виходить вона виграшна." "З позиції 3 можна перейти в позиції 0 і 1. Отже, вона теж виграшна." "З 4 можна перейти в 2 та 1 – виграшна. З 5 у 2 та 3 – програшна, тому що 2 та 3 виграшні. І з 6 перехід у 3 та 4. Вони виграшні, значить 6 предметів – це програшна позиція"
Навчальний	Але ми розібралися з грою, коли купка предметів – невелика (у нашому випадку – 6 рибок). Ми застосували ретроспективний аналіз. Але, якщо купка буде велика, то такий аналіз неефективний, потрібно використовувати теорію Шпрага-Гранді.
Ігровий	Перегляд вікон 2. Функція mex, 3. Числа Гранді
Ігровий	Знову виводимо граф зі станами гри для 10 предметів.
Навчальний	"Будемо тепер виграшність позицій визначати за допомогою чисел Гранді, це в багатьох випадках зробить алгоритм більш ефективним. Починаємо зі станів, з яких уже нікуди не можна піти (0 та 1), у них числа Гранді дорівнюють 0, тому що це програшні стани. Наступні стани визначаємо, використовуючи функцію mex від множини значень Гранді по кожному переходу, звідки отримуємо min, яке не зустрічається серед цих значень. Відповідно отримуємо число Гранді поточного стану, яке говорить нам чи це виграшний стан, а саме, якщо число Гранді нульове, то програшне, інакше — виграшне."
Навчальний	"Уявити це у вигляді графа простіше. Тут G - числа Гранди." "Зі стану 2 можна перейти тільки в стан 0. G(2) = mex{0} = 1." "Зі стану 3 можна перейти в стан 0 і 1. Отже, G(3) = mex{0} = 1." "Вкажи наступні значення чисел Гранді для всіх станів, що залишилися."
Ігровий	Виводимо поля для заповнення чисел Гранді для кожної позиції. Перевіряємо введені значення.
Навчальний	"Числа Гранді для деяких ігор можуть мати період."
Ігровий	Перегляд вікна «4. Закономірності в числах Гранди». Вивід графу зі станами гри і відповідним числами Гранді для них.
Навчальний	"Можна побачити, що в числах Гранді для цієї гри є закономірність, а саме, період: 0, 0, 1, 1, 2. Оскільки періоді чисел 5, то визначення виграшності позиції потрібно знайти залишок від розподілу кількості предметів у купці на 5. Якщо залишок дорівнює 0 чи 1, це програшна позиція. А якщо решта дорівнює 2, 3 або 4, то це виграшна - хто ходить, той виграє. Звичайно, якщо правильно ходить.
Навчальний	"А як правильно ходити?" "Як ми вже знаємо, потрібно ходити так, щоб своїм ходом зробити програшну позицію для іншого гравця. Потрібно взяти стільки предметів (2 або 3), щоб залишок від поділу на 5, отриманий після взяття предметів, дорівнював 0 або 1." "Тобто, якщо початковий залишок дорівнює 2, то взяти 2 предмети; якщо 3, то 3 або 2 предмети; якщо 4, то 3 предмети."

У табл. 4 наведені елементи ігрового сценарію, що об'єднує навчальні та ігрові дії, і реалізує таким чином модель навчального сценарію з елементами гри «НІМ з обмеженнями для декількох купок».

Таблиця 4

Опис елементів сценарію гри «НІМ з обмеженнями для декількох купок»

Сценарій	Зміст елемента
Навчальний	"Як і раніше, розглядаємо гру, коли з однієї купки можна взяти 2 або 3 предмети". Як приклад розглянемо гру з трьома купками 7. 5 та 4 предмети відповідно. "Для рішення гри НІМ з обмеженнями для декількох купок вводять поняття суми ігор".
Ігровий G	Перегляд вікна «Ігри з кількома купками на основі концепції суми ігор»

продовження таблиці 4

Навчальний	"Потрібно визначити, чи ця позиція є виграшною. Якщо так, то при оптимальній грі перший гравець виграє. Якщо ця позиція - програшна, то при оптимальній грі перший гравець програє."	
Навчальний	"Спочатку вважаємо числа Гранді G для кожної купки, і якщо купок три, потім знаходимо G = G1 XOR G2 XOR G3. Якщо G>0, то позиція - виграшна, інакше якщо G = 0 - то програшна."	
Навчальний	"Для кожної купки знаходимо G. Для цього 7, 5 і 4 ділимо на 5, і беремо залишок від поділу (бо значення числа Гранді для цієї гри мають період з 5 чисел). Якщо залишок дорівнює 0 або 1, то G = 0 Якщо залишок дорівнює 2 або 3, то G = 1. Якщо 4, то G = 2."	
Ігровий	Виводимо поля для заповнення значень G1, G2 та G3. Перевіряєм введені значення.	
Навчальний	"Підрахуємо значення G для суми ігор."	
Ігровий	Виводимо поле для заповнення значення G = G1 XOR G2 XOR G3. Перевіряєм введене значення.	
Навчальний	"У нас "виграшна позиція. Ми вже знаємо, що потрібно, щоб у другого гравця вийшла позиція, для якої G=0. Значить находимо в цій сумі, в двійковому коді , місто старшої одиниці. Знаходимо купку , в якій є одиниця в тій самій же позиції." "Це (номер - х) купка - (двійкове уявлення)."	
Навчальний	"Порахуй XOR-суму S і розмір знайденої купки – одержуємо кількість предметів, яку потрібно залишити у знайденій купці при оптимальному ході." "Введи в поле:<поле>"	
Ігровий	Вивід поля для вводу числа	
Навчальний	"Правильно. Можеш ходити."	Неправильно. Хочеш ще раз пройти навчання?
Ігровий	Кнопки: "Продовжити навчання" та "Повернутись"	
Навчальний	"Добре. Але обмеження можуть бути різні. Ми розглянули випадок з 2 або 3. Для різних обмежень потрібно шукати свої значення чисел Гранді та періодичність." "Візьмемо обмеження 2 і 4. Визнач значення чисел Гранді."	
Ігровий	Виводимо граф та поля для заповнення значень. Перевіряєм введені значення.	
Навчальний	"Правильно. Яка періодичність функції Гранді?"	"Ні ти помилився."
Ігровий	Виводимо поле для заповнення значення періодичності. Перевіряєм введене значення.	Кнопки: "Спробувати" та "Дізнатися результат"
Навчальний	"Правильно."	"Ні ти помилився. Хочеш спробувати ще раз?"
Навчальний	"Спробуй тепер зіграти в гру, де ти можеш взяти або 2 або 4 предмети."	
Ігровий	Створюється гра з 6, 4, 3 предметами	
Навчальний	“Задані 3 купки рибок. Можна брати 2 чи 4 рибки. Хто виграє при оптимальній грі?”	
Ігровий	Кнопки: “Спробувати власноруч” та “Як виграти”	
Навчальний	"Можеш скористатися блокнотом"	Перехід до режиму підказок

Сценарій для гри Дати. У таблиці 5 наведені елементи ігрового сценарію, що об'єднує навчальні та ігрові дії, і реалізує таким чином модель навчального сценарію з елементами гри для гри «Дати».

Таблиця 5

Опис елементів ігрового та навчального сценарію гри «Дати»

Сценарій	Зміст елемента
Навчальний	Гра Дати відноситься до гри, де для визначення виграшної стратегії застосовується ретроспективний аналіз. "Тобто для кожної позиції в грі заздалегідь необхідно визначити виграшна вона чи ні. "Візьмемо поширений варіант гри, коли кінцевою датою є 31 грудня." "Для першого гравця дата 31 грудня є програшною." "Оскільки гравці під час ходу можуть збільшувати день чи місяць на 1 або 2, то можливий перехід у дати 30.12, 29.12 та 31.10 (дати 31.11 не існує)"

продовження таблиці 5

Навчальний	"З алгоритму знаємо, що з якоїсь позиції всі ребра ведуть у виграшні позиції, то ця позиція програшна". "Отже, позиція 30.12 та 31.10 – програшні для першого гравця. А 29.12 виграшна, оскільки з неї можна перейти о 30.12".	
Ігровий	Позначаємо на ігровому полі розглянуті дати відповідним кольором (позначкою).	
Навчальний	"Візьмемо наступну дату – 28.12. Ми можемо з неї перейти о 29.12 та 30.12" "З алгоритму знаємо, що якщо з якоїсь позиції є ребро в програшну позицію, то ця позиція виграшна." "Тоді вершина 28.12 - виграшна (30.12 - програшна)"	
Ігровий	Позначаємо на ігровому полі розглянуту дату 28.12 відповідним кольором (позначкою).	
Навчальний	Візьмемо наступну дату - 27.12. Ми можемо з неї перейти в 29.12 і 28.12" "З алгоритму знаємо, що якщо з якоїсь позиції всі ребра ведуть у виграшні позиції, то ця позиція програшна" "Тоді вершина 27.12 - програшна (28.12-29.12 - виграшні)"	
Ігровий	Позначаємо на ігровому полі розглянуту дату 27.12 відповідним кольором (позначкою).	
Навчальний	"Візьмемо дату - 30.11. Ми можемо з неї перейти в 30.12" "З алгоритму знаємо, що якщо з якоїсь позиції є ребро у програшну позицію, то ця позиція є виграшною." "Тоді вершина 30.11 - виграшна (30.12 - програшна)"	
Ігровий	Позначаємо на ігровому полі розглянуту дату 30.11 відповідним кольором (позначкою).	
Навчальний	"З дати 29.11 можемо перейти в 29.12 і 30.11" "З алгоритму знаємо, що якщо з якоїсь позиції всі ребра ведуть до виграшних позицій, то ця позиція програшна" "Тоді вершина 29.11 - програшна (29.12,30.11 - виграшні)"	
Ігровий	Позначаємо на ігровому полі розглянуту дату 29.11 відповідним кольором (позначкою).	
Навчальний	"Отже ти бачиш, що, розглядаючи позиції, ми рухаємося, поступово зменшуючи дати. Тобто розглядаючи якусь дату, нам потрібно розуміти, в які позиції ми можемо перейти з неї, для того щоб визначити виграшність або програшність дати, що розглядається".	
Навчальний	"Спробуй далі сам визначити, якою є позиція для дати 26.10. Але ти маєш визначити на початку всі наступні від дати 26.10 позиції." "У разі потреби ти можеш переглянути алгоритм ретроспективного аналізу." "Вибери дату."	
Ігровий	Виводимо кнопку для перегляду алгоритму. Натискаючи на неї, користувач може переглянути алгоритм визначення позиції. Очікуємо вибору дати.	
Ігровий	Користувач обрав дату, з якої не усі наступні дати розглянуті.	Користувач обрав коректну для перегляду дату. Користувач визначає, якою є виграшність цієї дати.
Навчальний	"Потрібно розглянути попередні дати"	Виводяться відповідні повідомлення про правильність вибору.
Ігровий	Користувач визначає позицію дати - 26.10.	
Навчальний	"Ми розглянули 31 грудня як кінцеву дату. Якщо взяти іншу дату, то стратегія не змінюється, тільки треба рухатись назад від цієї дати" "Візьмемо кінцеву дату – 29.11 та початкову – 15.08."	
Навчальний	"Визнач виграшність позицій від дати 29.11 до 15.08, тобто у зворотному порядку."	
Ігровий	Користувач визначає виграшність вказаних позицій.	
Навчальний	"Добре. А тепер виходячи з розмітки кожної позиції, ти можеш формувати стратегію своїх переходів. Спробуємо зіграти в гру з комп'ютером, і на основі твоєї розмітки, слідуючи стратегії, ти можеш досягти перемоги." "Вибери початкову дату"	
Ігровий	Користувач обирає початкову дату 15.08. Створюється гра з комп’ютером, починаючи з обраної дати до 29.11. Користувач робить крок. Комп’ютер робить крок у свою чергу. При закінченні гри виводиться результат.	
Навчальний	"Вітаю, ти освоїв стратегію гри в Дати."	"Ти неправильно застосував стратегію, потрапив у програшну позицію і не зміг виграти."

Узагальнена методика для навчання комбінаторним іграм. Методика навчання користувача теорії комбінаторних ігор базується на сценаріях навчання для розглянутих ігор і є їх узагальненням.

I. Ознайомлення з теорією комбінаторних ігор

II. Попередня підготовка до гри: ознайомлення з правилами, вибір параметрів гри; наступні 3 пункти виконуються при необхідності під управлінням вчителя; побудова невеликої частини графа гри, починаючи з початкових вершин; розмітка вершин графа, тобто визначення виграшності або програшності для кожної вершини; виявлення закономірностей в розмітці вершин (якщо вони є). Наступні пункти виконуються для навчання гравця, як правильно ходити під час гри.

III. Вироблення правильного ходу (під керівництвом системи або самостійно): знаходження типу поточного стану гри (виграшна/програшна); обчислення правильного ходу, щоб перевести супротивника у програшний стан (якщо це можливо)

IV. Контроль правильності ходу користувача: попередження про неправильний хід; попередження про невірне введення даних; якщо користувач погодився на допомогу, то виконується пункт V.

V. Підказки по ходу гри: виграшність позицій – виграшна чи програшна; як визначається виграшність кожної поточної позиції та як зробити правильний хід (див. пункт III); як рахувати XOR-суму та числа Гранді.

Проектування та випробування програмної системи для навчання теорії комбінаторних ігор. Далі представлено UML діаграму варіантів використання, на основі якої спроектовано систему навчання комбінаторним іграм (рисунок. 2). Таким чином, гравець може почати гру, вибравши тип та параметри, переглянути минулі ходи, скористатися блокнотом для обчислень. Під час гри одержує навчальні матеріали про комбінаторні ігри взагалі, а також “НІМ”, “НІМ з обмеженнями” та “Дати”; проводить партії з системою, при цьому одержує підказки по ходу гри згідно з розробленими сценаріями.

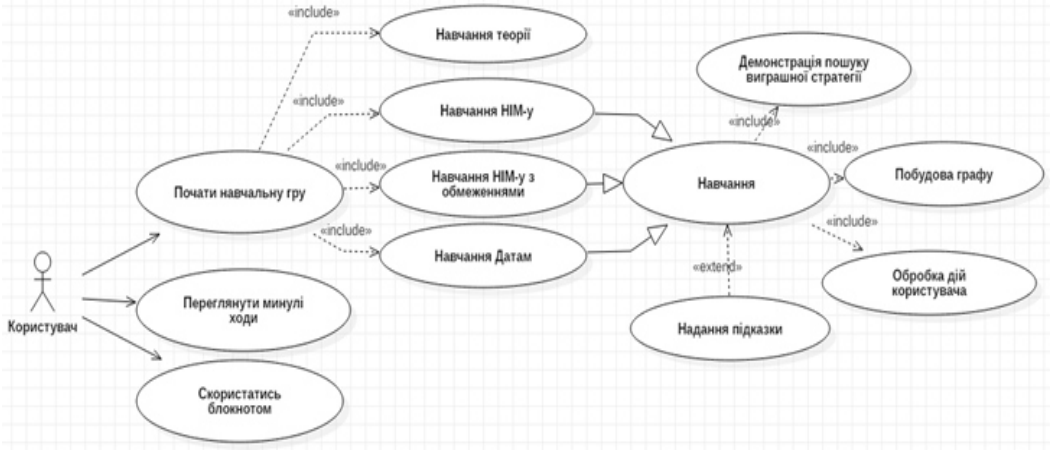


Рис. 2. Діаграма варіантів використання системи навчання комбінаторним іграм

При реалізації системи одним із доцільних варіантів є використання інструментальних засобів, як Unity3D/C#.

Навчання іграм за допомогою навчальної програмної системи. В якості предметів в купках вибрані рибки, в забирає рибок з купок — кошеня. Під час гри звучать легкі звуки природи біля озера. Коли вибираємо рибок, спрацьовує звук плескоту риби. І є звукові доріжки в кінці гри, які сигналізують про перемогу або поразку.

Гра “НІМ”. Починаючи гру, користувач проходить попередню підготовку. Спочатку показуються вікна з теорією про комбінаторні ігри, а також про гру НІМ. Потім розглядаються різні ігрові позиції. Наприклад, для гри зі станом – 3, 2 та 1 рибка у купках відповідно - це наступні {2,2,1}, {2,2}, {2}, {1} та інші. Ці всі позиції показують користувачу у вигляді списку, а також автоматично будується

орієнтований граф гри, де вершини – це всі позиції, а ребра показують всі можливі переходи між позиціями (рисунок 3). та користувач розмічає граф, тобто визначає виграшність або програшність для указаних вершин (станів гри). Після цього програмна система перевіряє правильність відповідей.

В режимі навчання після попередньої підготовки ведеться гра згідно зі сценарієм, показаним в таблиці. 2. Система допомагає користувачу спочатку визначити, чи є позиція для нього виграшною або програшною. І якщо вона виграшна, то веде його вздовж гри, щоб він грав оптимально, на деяких кроках підказує, на деяких перевіряє дії користувача.

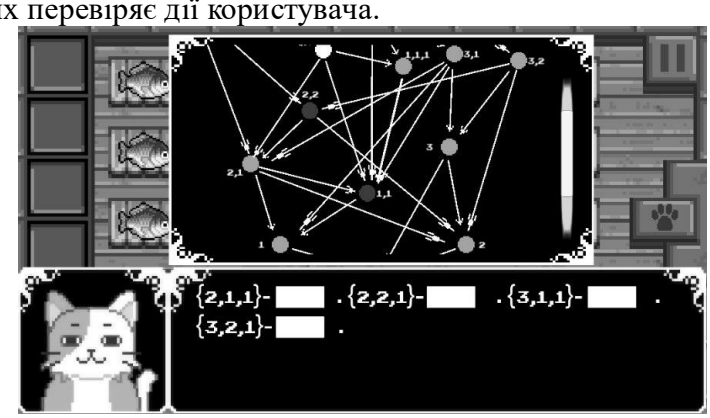


Рис. 3. Користувач розглядає граф гри та вводить виграшність вказаних позицій

Гра "НІМ з обмеженнями для однієї купки". Починаючи гру, користувач проходить попередню підготовку: показується вікно з теорією Шпраха-Гранді; потім показується гра з однією купкою, в якій, наприклад, 6 рибок, і визначається, що можна брати з купки тільки 2 або 3 рибки; для цієї гри автоматично будується граф, аналогічно, НІМ, тільки стани та переходи між ними інші. Далі визначається оптимальна стратегія гри, для цього користувач розраховує числа Гранді для станів гри, починаючи з початкових позицій, та вводить у зазначені полі їх значення (рисунок 4), а система їх перевіряє; якщо є закономірності у ряді чисел Гранді, то система просить у користувача звернути на це увагу.

Далі, згідно сценарію навчання (таблиця 3), гравець на основі числа Гранді визначає виграшність позиції, робить хід, і система відстежує оптимальність гри та дає підказки.

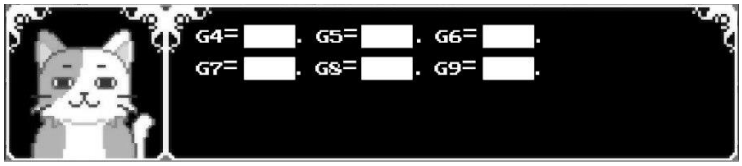


Рис. 4 Користувач розглядає граф гри та розраховує числа Гранді

Гра "НІМ з обмеженнями для декількох купок". Починаючи гру, користувач проходить попередню підготовку: показується вікно з теорією про суму ігор; потім показується гра з трьома купками, в яких, наприклад, 7, 5 і 4 рибки відповідно, і визначається, що можна брати з купки тільки 2 або 3 рибки. Далі визначається оптимальна стратегія гри. Спочатку, згідно сценарію навчання (таблиця 4), визначається виграшність позиції, для цього користувач розраховує числа Гранді для кожної купки та їх XOR-суму. Гравець робить хід, у випадку виграшної позиції система відстежує оптимальність гри та дає підказки.

Гра "Дати". Починаючи гру, користувач проходить попередню підготовку: показується вікно з теорією ретроспективного аналізу ігор; потім показується гра у вигляді календаря для одного місяця, наприклад, грудня (рисунок 5), тому що кінцева дата - 31 грудня. Далі гравець, згідно сценарію в таблиці 5, визначає

початкову дату та за допомогою системи визначає виграшність для першого гравця всіх позицій від останньої до початкової за умови, що під час ходу можна збільшувати на 1 або 2 або день на місяці, або місяць, але не те й інше відразу. На рис. 6 зображено результати визначення виграшності декількох дат, починаючи з кінцевої 31 грудня. Червоним позначено програшні дати для першого гравця, зеленим – виграшні.

З цього моменту вже починається гра, і гравець її проводить згідно із заздалегідь визначених властивостей дат, а саме їх виграшності.

Рис. 5. Користувач визначає виграшність дат

Висновки. Розроблено узагальнену методику для навчання математичної теорії комбінаторних ігор, що включає систематизацію учбового курсу про комбінаторні ігри та навчальні сценарії з елементами гри для “НІМ”, “НІМ з обмеженнями” і “Дати”.

Навчальна комбінаторна гра позиціонується як трансляція освітнього повідомлення для загальної аудиторії гравців. Ціль гравця в такій системі полягає в отриманні теоретичних відомостей – інформації, а також вдосконалення навичок гри – дії. За наявністю ігрового сюжету гра відноситься до ігор, що засновані на правилах. Гра ведеться в реальному часі та розрахована на одного гравця. Інтерфейс користувача з отримання ігрової інформації складається з елементів 2D графіки. При передачі даних до гри використовується штучний інтерфейс, а саме позиційний пристрій типу “миша” або Touchpad.

Створена методика випробувана при реалізації вищезгаданих ігор. Система впроваджена в клієнтську програмну частину продукту «Game of Strategy», яка є комп'ютерною настільною грою для організації процесу навчання математичної теорії ігор, визначення виграшної стратегії, стеження за грою користувача, надання допомоги та підказок. Також реалізовано можливість перегляду минулих ходів та можливість робити підрахунки у блокноті під час гри.

Розроблена методика може бути використана як для самостійного навчання, так і для гібридного, коли студент слухає лекції на тему, а потім для кращого засвоєння матеріалу використовує розроблену систему. Для викладання матеріалу на цю тему викладачу необхідно 8 лекцій (16 годин) для викладання теорії та 4 практичних занять (8 годин + 8 годин самостійної роботи) для його засвоєння, тобто опанування теоретичного матеріалу і опробування цих знань у грі, всього 24 години. Згідно з результатами проведеного експериментального випробування у гібридному режимі, коли студенти застосовували систему тільки для практичних зайняття та самостійної роботи, застосування розробленої програмної системи дозволило скоротити час у середньому до 8 годин, тобто в 2 рази.

Надалі планується доопрацювання наявних сценаріїв навчання з елементами гри, додавання ігрової частини сценаріїв більшої гнучкості, поділ їх на модулі, додавання іншого типу взаємодії з користувачем замість інструментів Unity "User Interfaces", можливість будувати граф для кожної гри. Відповідно, зробити ще зручнішим та зрозумілішим сценарії навчання.

Список літератури

1. Чурок С., Шамоня В. Використання комп'ютерних ігор в навчанні інформатики учнів основної школи. *Освіта. Інноватика. Практика*. 2022. 10(1). 60–70. https://doi.org/10.31110/2616-650X-vol10i1-007
2. Лугова Т.А. Блажко О.А. Проектування комп`ютерних ігор для навчання: навчальний посібник. Одеса: ФОП «Побута». 2018, 212 с. URL: https://bit.ly/3NPaoXZ
3. Lucas Chess. An easy way to play and train chess on your PC. URL: https://lucaschess.pythonanywhere.com/
4. Arena Chess GUI. URL: http://www.playwitharena.de/
5. Aurora Borealis: checkers database program URL: http://aurora.draughtsworld.com/
6. SmartGo One. Learn, play, study Go. URL:https://smartgo.com/
7. WZebra. Othello game. URL:http://radagast.se/othello/
8. Nim URL:https://en.wikipedia.org/wiki/Nim
9. Berlekamp E., Conway John H., Guy R. Winning ways for your mathematical plays / 2nd edition. 2001, 297 p. ISBN 1-56881-130-6
10. Ортинський В., Варій М. Основи психології і педагогіки. Львів: Центр навчальної літератури Львівська Політехніка, 2017. 548 с.
11. Іванченко Н. О., Подскребко О. С., Квашук Д. М. Проведення on-line лекцій ОПП «Цифрова економіка» ОПП «економічна кібернетика» з використанням технологій машинного зору /Дистанційна освіта в Україні: інноваційні, нормативно-правові, педагогічні аспекти: зб. наук. праць матеріалів І Всеукраїнської науково-практичної конференції, 16 червня 2020 р., м. Київ, Національний авіаційний університет / наук. ред. Н.П. Муранова. К. : НАУ, 2020, с. 47-49.
12. Szilagyi I., Roxin I. Model for Active Semantic Learning System. *Proceedings of the IADIS International Conference e-learning*. Freiburg, Germany 2010. V.2. P. 247 – 250.
13. Нікітін С.О., Нікітіна Л.О. Основи комп'ютерних ігор та ігрових програм: довідник модуля. Х.:Друкарня Мадрид, 2018. 138 с.
14. Chickerur S. Integrating Problem Based and Project Based Learning for Effective Teaching Learning in Engineering Education - A Case Study of Advanced Database Management Course. *Advanced Science and Technology Letters*. 2013. V.36. P.63-66.
15. Nutaro J. Building Software for Simulation: Theory and Algorithms, with Applications in C++. Hoboken, NJ: Wiley, 2010. P.13-21.
16. Sokolowski J.A., Banks C.M. Principles of Modeling and Simulation. Hoboken, NJ: Wiley. 2009, 6 p.
17. Hainey T., Connolly T., Boyle L. Evaluation of a Game to Teach Requirements Collection and Analysis in Software Engineering at Tertiary Education Level. *Proceedings of the 3rd European Conference on Games-Based Learning*. Graz, Austria. 2009. P. 145 - 153.

В.М. Рувінська, А.С. Тройніна

INFORMATION TECHNOLOGY FOR TRAINING THEORY AND PRACTICE OF COMBINATORIAL GAMES

V.M. Ruvinska, A.S. Troynina

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
emails: iolnlen@te.net.ua; anastasiyatroinina@gmail.com

The aim of the work is to reduce the time to study the theory and practice of combinatorial games through the development of a methodology and training system and integrate it into a computer training game that helps to build the correct strategy of the game, makes hints for the optimal move, allows you to conveniently observe the results of the games, review past moves, do mathematical calculations, herewith offering a unique and interesting design. As a result of the work, the training methodology and software product has been developed, which is a game that organizes the process of study the definition of winning strategies for each combinatorial game using the developed methodology and training system. The development tools are the Microsoft Visual Studio integrated development environment for programming in C#, a multi-platform tool for developing two-dimensional and three-dimensional games Unity3d, StarUML, as a tool for modeling business logic of an application and using version control system Git.
Keywords: teaching methodology, game and training script, training program, mathematical combinatorial theory of games, game strategy, winning position, losing position, XOR-sum.

DOI 10.15276/imms.v13.no3-4.311
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 311-321

МОДИФІКАЦІЯ МЕТОДУ ВИБОРУ КОНТЕЙНЕРА ДЛЯ ЗМЕНШЕННЯ ЧУТЛИВОСТІ СТЕГАНОПОВІДОМЛЕННЯ ДО ЗБУРНИХ ДІЙ

С.М.Сокальський

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: sokalskiyserhiy1@gmail.com

Питання захисту інформації від несанкціонованого доступу сьогодні є одним із ключових в сфері інформаційних технологій. Оскільки поширення цифрових технологій в усі сфери людської діяльності не зупиняться, і методи захисту інформації від небажаного доступу покращуються, то не зупиняється і розвиток методів та технологій отримання несанкціонованого доступу до конфіденційної інформації у зловмисних цілях. Тому важливо продовжувати вдосконалювати системи захисту інформації, тим самим перешкоджаючи зловмисникам. Складовою частиною будь-якої сучасної системи захисту інформації є стеганосистема, що забезпечує прихований канал передачі даних, який дозволить передавати інформацію, не викриваючи перед зловмисником факт її наявності. Задача вибору стеганографічного контейнера дозволяє вирішити деякі із вимог, що ставляться до стеганосистеми при її побудові. Однією із найважливіших вимог є забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення, адже такі атаки не вимагають від зловмисника обширних знань у галузі стеганографії та стеганоаналіза і не вимагають наявності спеціальних технічних засобів, що робить даний вид атак простим та розповсюдженим. *Метою* робити є підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, розробленого автором раніше, що забезпечить максимально можливу для аналізованих зображень, або близьку до максимальної, стійкість стеганоповідомлення до атак проти вбудованого повідомлення. Поставлена мета була досягнута шляхом модифікації кількісної оцінки об'єму захищеної інформації, а саме використанням відносного значення об'єму захищеної інформації до об'єму всієї вбудованої інформації. Результатом роботи є розробка модифікації методу вибору стеганографічного контейнера, що готовий до практичного застосування. Ефективність запропонованого методу є вищою ніж методу-прототипу, та залишається високою незалежно від того, який стеганометод чи збурення були використані. Значущість результату полягає у підвищені загальної стійкості стеганосистеми до атак проти вбудованого повідомлення за рахунок використання даного методу для вибору стеганоконтейнера.

Ключові слова: стеганосистема, стеганографічний метод, стійкість стеганосистеми, стеганографічний контейнер, цифрове зображення, сингулярні трійки.

Вступ. В результаті бурхливого розвитку комп'ютерних та інформаційних технологій процеси обміну, передачі та збереження конфіденційної інформації зайняли важливе місце у кожній сфері людської діяльності. Саме тому питання захисту цієї інформації від несанкціонованого доступу, зміни та спотворення є надзвичайно важливими.

Зараз тяжко уявити комплексну систему захисту інформації без стеганосистеми, мета якої при організації каналу зв'язку полягає у приховуванні самого факту наявності секретної інформації шляхом вбудовування цієї інформації у деякий інформаційний контент – контейнер, зазвичай цифровий [1-5], який не привертає уваги. Після вбудови приховуваної інформації отриманий контент повинен ніяк візуально не відрізнятися від контейнера, тобто зберігати

надійність сприйняття. Але із розвитком технологій захисту інформації також розвиваються і способи отримання несанкціонованого доступу до конфіденційної інформації, її зміни або знищення, тому завдання покращення методів прихованої передачі даних залишається актуальним і на сьогоднішній день.

Процес стеганографування умовно можна розділити на три етапи: вибір контейнера, попереднє кодування інформації, що передається, результат якого надалі називається додатковою інформацією (ДІ), і вбудовування ДІ у контейнер, в результаті чого отримується стеганоповідомлення. Контейнери можуть бути двох типів – потокові або фіксовані. Потокові контейнери представляють собою послідовність бітів, яка постійно змінюється в часі, і ДІ вбудовується в них у реальному масштабі часу. У такому випадку завчасно неможливо визначити обсяг інформації, яку можна буде вбудувати у контейнер, на відміну від фіксованого контейнера, що має чітко визначені характеристики, зокрема розміри. Саме при використанні фіксованих контейнерів є можливість завчасно обчислити обсяг інформації, яку можна вбудувати у контейнер. Враховуючи це, а також специфіку задачі, що розглядається в роботі, яка зазначається нижче, далі розглядаються фіксовані контейнери – цифрові зображення (ЦЗ).

При побудові стеганосистеми до неї висувається ряд вимог, серед яких забезпечення стійкості до атак проти вбудованого повідомлення, надійність сприйняття стеганоповідомлення, стійкість до стеганоаналізу, тощо [6,8]. На сьогодні саме стійкість стеганосистеми до атак проти вбудованого повідомлення, метою яких є внесення змін в стеганоповідомлення, наслідком чого може стати спотворення або навіть повне знищення вбудованої ДІ, вважається найбільш пріоритетною ціллю: на відміну від стеганоаналітичних атак, які, як правило, потребують спеціальних технічних та програмних засобів і високої кваліфікації атакуючого, атаки проти вбудованого повідомлення можуть проводитись без специфічного програмного або технічного забезпечення, без спеціальної підготовки та кваліфікації зловмисника, наприклад, атака стисненням, накладення шуму, фільтрація. Це робить такий вид атак надзвичайно простим і поширеним, і саме це диктує високу потребу у забезпеченні стійкості прихованого повідомлення до збурних дій.

При організації прихованого каналу зв’язку можуть бути використані випадкові, нав’язані або ж обрані контейнер. Саме обрані контейнери в більшій чи меншій степені дозволяють покращити властивості чи задовольнити вимоги, що висуваються до отримуваного стеганоповідомлення, залишаючи актуальною задачу їх вибору, розв’язку якої присвячена дана робота.

Питанням формування методу вибору контейнера з метою забезпечення певних вимог стеганоповідомлення займаються багато вчених-стеганографів. Так у [9] дані контейнера моделюються як процес Гауса-Маркова. Основною ціллю виступає забезпечення стійкості стеганосистеми до стеганоаналізу.

У роботі [6] піднімається питання забезпечення надійності сприйняття стеганоповідомлення та стійкості стеганосистеми до стеганоаналізу, але питання забезпечення стійкості до атак проти вбудованого повідомлення в [6,7] не розглядається.

У [10] вибір контейнера проводиться лише для одного стеганометода Бенгама-Мемона-Ео-Юнга. Таке значне обмеження для застосування цього методу робить його неможливим для розглядання у якості вирішення проблеми забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення в цілому.

У роботі [11] було представлено метод, що базується на основі поняття обсягу захищеної інформації, що кількісно визначає об'єм вбудованої інформації, яка є захищеною від деякої збурної дії. Значною перевагою цього методу є

відсутність обмежень на застосування стегнографічних алгоритмів і конкретики прогнозованих атак.

У роботі [12] запропоновано метод вибору стеганографічного контейнера на основі введеної кількісної характеристики, що характеризує об'єм інформації, яка буде правильно декодована після атаки на стеганоповідомлення, та обчислюється з врахуванням вектору розподілу ДІ серед власних векторів симетричної матриці контейнера та чутливості цих векторів до збурної дії *E*, що відображає збурення від прогнозованої атаки на стеганоповідомлення.

Цей метод базується на можливості представлення стеганоперетворення, тобто процесу вбудовування додаткової інформації, як деякої адитивної операції над матрицею ЦЗ-контейнера:

$$F = \overline{F} + \Delta F \tag{1}$$

де F - n×n-матриця контейнера, $\overline{F}$ - матриця СП, ΔF - n×n-матриця збурення, яке виникло в результаті вбудовування ДІ у контейнер. У роботі введене поняття захищеної від збурної дії E інформації, де E – матричне представлення збурної дії, що виникла в процесі атаки проти вбудованого повідомлення. Але, як показала практика, між об'ємом захищеної інформації (ЗІ), розрахункова формула якого запропонований в роботі, і обсягом правильно декодованої інформації систематична відповідність відсутня. Крім того викликає сумніви доцільність використання при розрахунках ЗІ спектру матриці контейнера та її власних векторів. Оскільки для отримання цих параметрів необхідно спочатку виконати процес симетризації матриці контейнера, то цей набір параметрів однозначно визначає не первісну матрицю контейнера, а її специфічну модифікацію. З урахуванням вищенаведеного у роботі [13] присвяченій задачі, що розглядається, цей набір параметрів був змінений на сукупність сингулярних векторів і сингулярних чисел $n \times n$-матриці контейнера F (довільної структури), які можна отримати за допомогою нормального сингулярного розкладу:

$$F = U\Sigma V^T \tag{2}$$

де U, V - ортогональні $n \times n$-матриці, стовпці яких u_i, v_i, $i = \overline{1,n}$, є лівими та правими сингулярними векторами (СНВ) відповідно, при цьому ліві СНВ додатково є лексикографічно додатними; $\Sigma = diag(\sigma_1, ..., \sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ – сингулярні числа (СНЧ) F. СНЧ довільної F, як і власні значення симетричної матриці, є добре обумовленими через співвідношення [19]:

$$\max_i \left|\sigma_i(F) - \sigma_i(F+E)\right| \leq \|E\|_2 \tag{3}$$

де $\|\cdot\|_2$ – спектральна матрична норма, E – n×n матриця збурення, мірою ж чутливості до збурень СНВ u_i досі вважалася відокремленість

$$svdgap(i,F) = \min_{i \neq j} \left|\sigma_i - \sigma_j\right| \tag{4}$$

відповідного СНЧ σ_i згідно з формулою:

$$\sin 2\theta_i \leq 2\|E\|_2 / svdgap(i,F) \tag{5}$$

де θ_i - кут повороту u_i в результаті збурної дії E. Очевидно, що співвідношення (5) дає оцінку зверху для кута θ_i тільки тоді, коли його права частина менше чи дорівнює 1. Інакше поведінка вектора u_i після атаки непередбачувана. Для визначення «контрольованих» формальних параметрів (СНВ) в [13] було введено поняття СНЧ σ_i матриці F, яке має достатню відокремленість щодо збурної дії E. Для такого СНЧ має місце співвідношення:

$$svdgap(i,F) \geq 2\|E\|_2 \tag{6}$$

при цьому відповідний СНВ u_i називається захищеним від збурної дії E.

Для формування методу вибору контейнера з сукупності даних, що забезпечить максимальну (близьку до максимальної) стійкість відповідного

стеганоповідомлення до атак проти вбудованого повідомлення, в [13] було введене поняття поля, що захищене від збурення E, яке являє собою суму однорангових матриць, кожна з яких відповідає сингулярній трійці (σ_i, u_i, v_i) де СНЧ має достатню відокремленість стосовно збурення E, тобто є малоранговою апроксимацією матриці контейнера. Опираючись на це, було запропоновано формулу для обчислення об'єму захищеної від E інформації, яка стала основою відповідного методу:

$$S = \left\| \sum_{k=1}^{m} \overline{\sigma_k} \cdot \overline{u_k} \cdot \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k \cdot u_k \cdot v_k^T \right\| \quad (7)$$

де m – максимальний індекс серед СНЧ F, які мають достатню по відношенню до E відокремленість, $(\overline{\sigma}_i, \overline{u}_i, \overline{v}_i)$ - сингулярні трійки матриці стеганоповідомлення. Формула (7) являє собою інформацію, що була вбудована у захищене поле контейнера і визначається як різниця малорангових апроксимацій матриці контейнера та стеганоповідомлення.

Запропонований в [13] метод є ефективнішим за наявні аналоги, але він не гарантує систематично вибір контейнера, що забезпечує максимально можливу стійкість відповідного стеганоповідомлення до збурень.

Мета статті та постановка досліджень. Метою роботи є підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, запропонованого в [13].

Під ефективністю стеганосистеми розуміється її стійкість до атак проти вбудованого повідомлення, що кількісно оцінюється значенням коефіцієнта кореляції NC між вбудованою ДІ, що представляє бінарну послідовність $p_1, p_2, \dots p_t, p_i \in \{0,1\}, i = \overline{1,t}$, та декодованою $\overline{p_1}, \overline{p_2}, \dots \overline{p_t}, \overline{p_i} \in \{0,1\}, i = \overline{1,t}$, ДІ [23]:

$$NC = \frac{\sum_{i=1}^{t} p_i' \times \overline{p_i'}}{t} \quad (8)$$

де $p_i' = 1, \bar{p}_i' = 1$, якщо $p_i = 1, \bar{p}_i = 1$, і $p_i' = -1, \bar{p}_i' = -1$, якщо $p_i = 0, \bar{p}_i = 0$.

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Модифікувати кількісну оцінку об'єму захищеної інформації, що є основою для модифікації методу [13] вибору стеганографічного контейнера;
2. Провести оцінку ефективності, зокрема порівняльну, модифікованого методу вибору контейнера.

Об'єктом дослідження є процеси забезпечення певних характеристик стеганоповідомлень при організації прихованого каналу зв'язку.

Предметом дослідження є методи вибору контейнера з заданої скінченної сукупності можливих, якому відповідає стеганоповідомлення, що має максимально можливу/близьку до максимально можливої стійкість до атак проти вбудованого повідомлення.

Основна частина. Оскільки будь-яке стеганоперетворення можна представити як деяке збурення матриці ЦЗ-контейнера згідно із формулою (1), то формально ДІ, яка вбудовується, можна представити у вигляді матриці збурення ΔF, та вирахувати за формулою:

$$\Delta F = \overline{F} - F \quad (9)$$

де F – матриця ЦЗ контейнера, $\overline{F}$ - матриця ЦЗ стеганоповідомлення. Очевидно, що в загальному випадку навіть при одній і тій самій ДІ, яка вбудовується одним і тим самим стеганометодом, але в різні ЦЗ-контейнери, формальне представлення ДІ, що отримується за допомогою (9), буде різним.

У методі, що представлений у роботі [13], згідно до формули (7) об'єм ЗІ вираховується як норма матриці різниці малорангових апроксимацій матриць ЦЗ контейнера та стеганоповідомлення, а це значить, що на об'єм ЗІ впливає не лише кількість СНЧ, що мають достатню відокремленість по відношенню до збурної дії, що задовольняє співвідношення (6), але й збурення, що матриця контейнера отримує внаслідок вбудовування ДІ.

Крім того, поняття достатньої відокремленості СНЧ (6), а також відповідного захищеного СНВ вводиться по відношенню до збурення E. Використовувана кількісна оцінка збурення, яке скрізь ((3), (5), (6)) фігурує у вигляді матричної норми $\|E\|_2$, буде залежати від розміру матриці E, тобто від розміру матриці ЦЗ-контейнера: чим більше розмір матриці, тим більше $\|E\|_2$, що підтверджується результатами обчислювального експерименту, наведеними на рис.1.

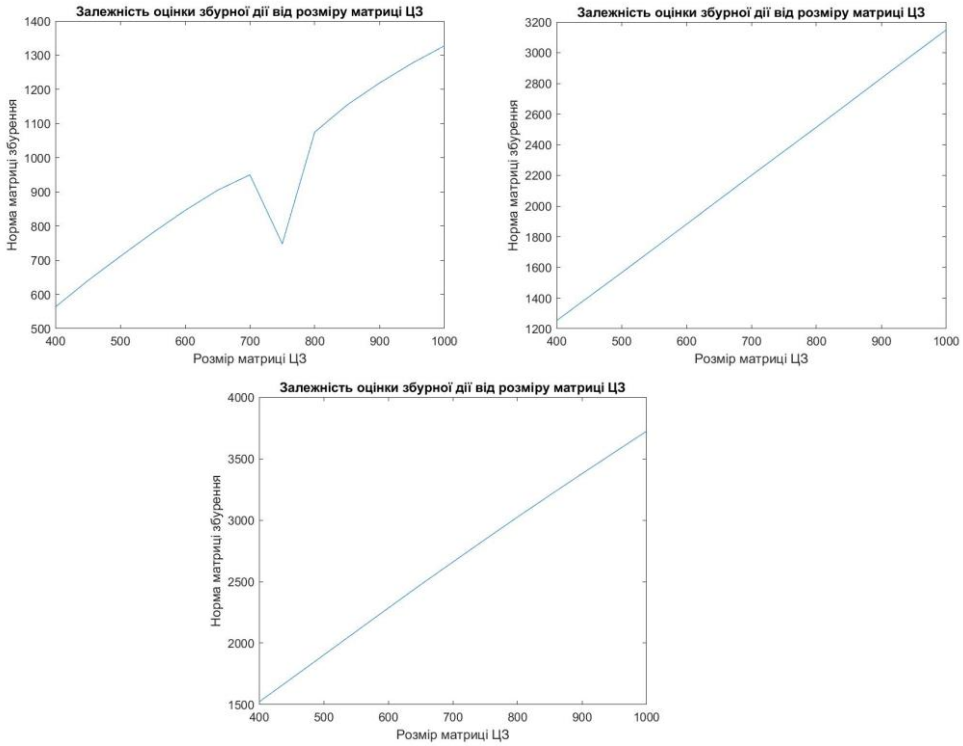


Рис.1. Залежність $\|E\|_2$ від розміру матриці ЦЗ, коли E відповідає: 1 – стиску ЦЗ з втратами з QF=75; 2 – накладанню гауссівського шуму з нульовим математичним очікуванням і D=0.001; 3 – накладанню пуассонівського шуму

Але ж конкретика збурення, характеристики атаки проти вбудованого повідомлення (стиску з втратами, накладання шуму, фільтрація, розмиття тощо), тобто її вид, властивості, зокрема «сила», ніяк не залежить від розміру того контенту, на який вона спрямована, зокрема ЦЗ, а визначаються параметрами цієї збурення (коефіцієнтом якості QF – стиск з втратами, математичним очікуванням і дисперсією – накладання шуму тощо).

СНЧ з достатньою відокремленістю – це m найбільших за значенням СНЧ [13]. Збільшення розміру ЦЗ, як правило, приводить до збільшення значення максимальних СНЧ. Дійсно, енергія $N(F)$ ЦЗ з $n\times n$-матрицею F з елементами f_{ij} може бути обчислена у відповідності з формулою [13]:

$$N(F)=\sum_{i,j=1}^{n} f_{ij}^2=\sum_{i=1}^{n}\sigma_i^2 \qquad (10)$$

Зі зростанням *n* трендом тут буде зростання $\sum_{i,j=1}^{n} f_{ij}^2$ і, як витікає з формули (10), зростання $N(F)$, а, враховуючи співвідношення між СНЧ матриці оригінального ЦЗ, а саме: $\sigma_1 >> \sigma_2 \geq ... \geq \sigma_n$, очікуваним є збільшення найбільших СНЧ *F*. Ці зміни ніяк не пов'язані з процесом, що розглядається, тобто зі збуреннями, що застосовуються до зображень в процесі стеганоперетворень та атак проти вбудованого повідомлення, але вони відіб'ються певним чином на складових формули (7).

З урахуванням вищенаведеного коректне використання формули (7) для порівняння властивостей контейнерів в однакових умовах їх використання вимагає, крім іншого, того, щоб всі ЦЗ, що претендують на роль контейнера, мали однакові розміри, але на практиці це, як правило, не виконується.

Для зменшення впливу наведених негативних факторів пропонується модифікувати розрахункову формулу (7) об'єму ЗІ наступним чином:

$$S = \frac{\left\| \sum_{k=1}^{m} \overline{\sigma_k} \cdot \overline{u_k} \cdot \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k \cdot u_k \cdot v_k^T \right\|}{\left\| \overline{F} - F \right\|} \qquad (11)$$

Формула (11) за змістом умовно надає відносну кількість ЗІ відносно ДІ в її конкретному для даного ЦЗ представленні і є основою для модифікованого методу вибору контейнера, що забезпечує максимальну/близьку до максимальної стійкість відповідного стеганоповідомлення до атак проти вбудованого повідомлення, основні кроки якого наступні.

Нехай *K* – задана множина ЦЗ-контейнерів, з яких відбувається вибір, $p_1, p_2 ... p_l$ - бінарна послідовність – результат попереднього кодування повідомлення, що пересилається, M_S - обраний для застосування ДІ стеганометод, *E* – формальне представлення передбачуваної атаки проти вбудованого повідомлення.

Крок 1. Для кожного ЦЗ $F \in K$:

1.1. Виконати вбудовування ДІ $p_1, p_2 ... p_l$ за допомогою вибраного стеганографічного методу M_S в контейнер *F*. Результат – СП з матрицею $\overline{F}$;

1.2. Побудувати нормальне сингулярне розкладання (2) для *F*;

1.3. Визначити відокремленості (4) для отриманих СНЧ;

1.4. Визначити множину *M* індексів СНЧ з достатньою відокремленістю по відношенню до збурення *E*;

1.5. Побудувати нормальне сингулярне розкладання (2) для $\overline{F}$;

1.6. Вирахувати відносне значення об'єму ЗІ *S* за формулою (11);

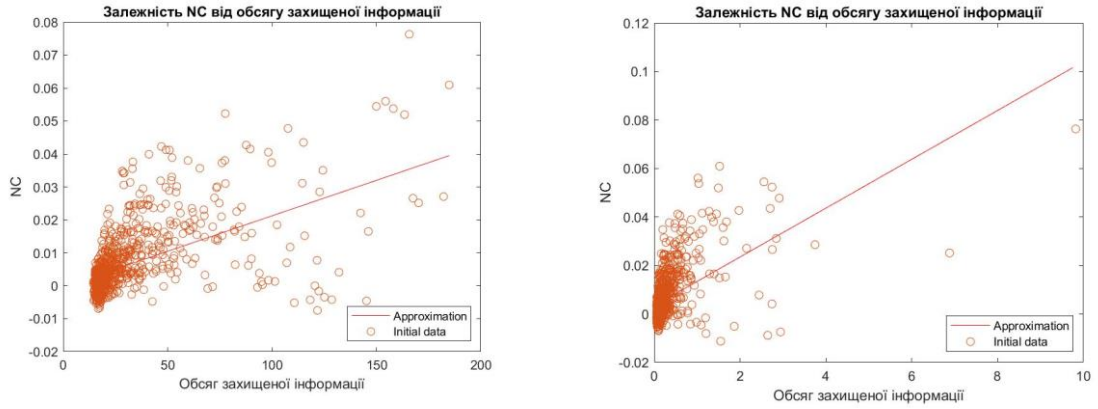
Крок 2. Серед всіх ЦЗ множини *K* визначити таке F_V, для якого відносне значення об'єму ЗІ $S(10)$ відповідатиме відношенню $S_V = \max_{F \in K} S$, ЦЗ F_V - шуканий контейнер.

Оцінка ефективності модифікованого методу вибору контейнера. Для оцінки ефективності модифікованого методу вибору стеганографічного контейнера було проведено обчислювальний експеримент, в ході якого були використані стеганометоди: Жао і Коха [14], модифікації найменшого значущого біта (LSB) [15], а також методи запропоновані у роботі [16] та [17]). В якості атак проти вбудованого повідомлення розглядалися: накладання мульиплікативного та гауссівського шумів з різними параметрами, атака стисненням з різними коефіцієнтами якості. Кінцева сукупність контейнерів-претендентів була представлена 1000 цифровими зображеннями формату .jpg та розміром 400x400

пікселів, що були взяті із незалежного джерела [18] і 100 цифровими зображеннями зробленими на аматорську цифрову камеру розміром 400x400 пікселів.

Для оцінки ефективності запропонованого методу вибору стеганоконтейнера використовується, по аналогії з [13], різниця між NC (8) контейнера з найбільшим об'ємом захищеної інформації (11), та найбільшим NC з усієї вибірки контейнерів-претендентів.

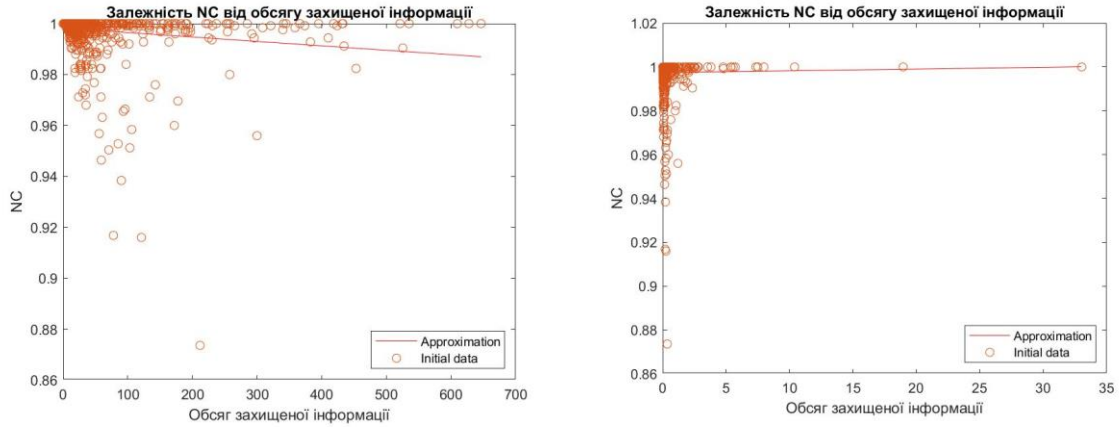
Деякі з результатів обчислювального експерименту відображені на рис.2-5.



а) б)

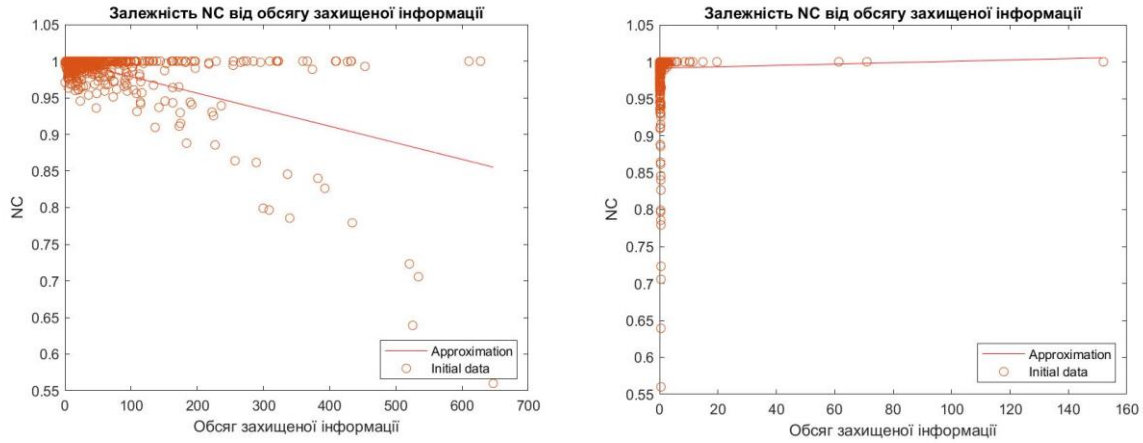
Рис. 2. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду LSB в умовах атаки стисненням з коефіцієнтом якості QF=85

На рис. 2 наглядно виражено залежність між NC та об'ємом захищеної інформації для цифрових зображень. І хоча пряма залежність відслідковується як і в випадку використання методу обчислення абсолютного значення об'єму захищеної інформації, так і в випадку обчислення відносного об'єму, але ефективність методів відрізняється: так у першому випадку NC, що відповідає цифровому зображенню з найбільшим абсолютним значенням об'єму захищеної інформації, становить 0,0609, а у другому випадку – 0,0763.



а) б)

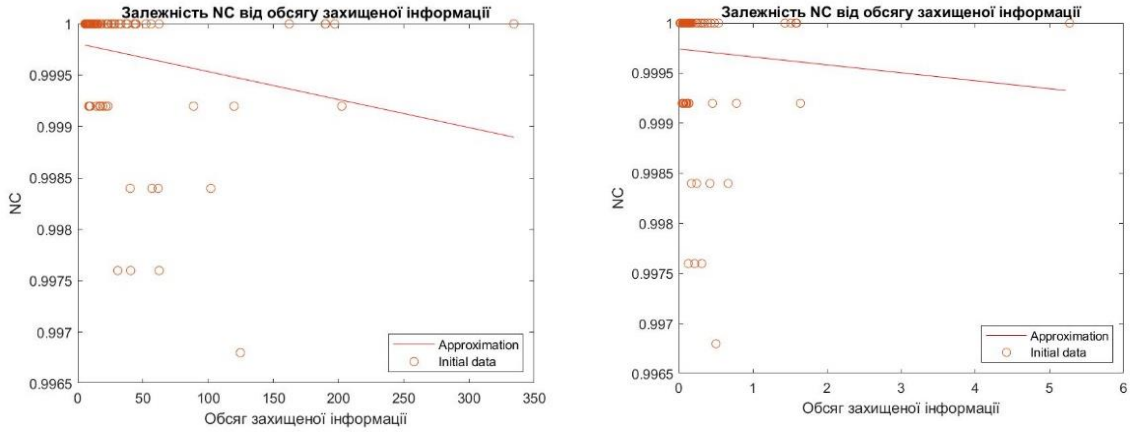
Рис. 3. Залежність NC від об'єму захищеної: а – методу [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха та атаки стисненням з QF=75



а) б)

Рис. 4. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха в умовах накладання мультиплікативного шуму з дисперсією 0,001

При чому максимальний NC з усієї вибірки становить 0,0763. Таким чином ефективність методу [13] в умовах використання стеганометода LSB та атаки стисненням з коефіцієнтом якості 85 становить 79,8 %, а методу представленого в цій роботі – 100%, що говорить про підвищення ефективності методу на 20,2 %.



а) б)

Рис. 5. Залежність NC від об'єму захищеної інформації: а – метод [13], б – метод, запропонований в роботі, з використанням стеганометоду Жао і Коха та атаки стисненням з *QF*=75, де в якості контейнерів-претендентів були використані ЦЗ зроблені на аматорську цифрову камеру.

З результатів, наведених на рисунках 2-5 випливає перевага запропонованого модифікованого методу в порівнянні з прототипом, яка підтверджується результатами, наведеними в табл.1.

Таблиця 1

Результати порівняльного аналізу запропонованого методу та методу [13]

Стеганометод	Збурення	Значення *NC*, що відповідає максимальному об'єму ЗІ		Максимальне значення NC в умовах експерименту
		Метод [13]	Наш метод	
Метод LSB (просторова область вбудовування ДІ) [15]	Стиснення з втратами, *QF*=75	0.0864	0.0985	0.0985
	Гауссівський шум с матоочікуванням 0 і *D*=0.000001	0,9007	0,9007	0,9241

продовження табл.1

	Мультиплікативний шум с *D*=0.000001	0.9993	0.9993	0.9993
Метод з кодовим управлінням вбудовування ДІ (просторова область вбудовування ДІ) [16]	Стиснення з втратами, *QF*=75	1	1	1
	Гауссівський шум з матоочікуванням 0 і *D*=0.0005	0.4856	1	1
	Мультиплікативний шум с *D*=0.0005	0.4920	1	1
Метод модифікації максимального СНЧ (вбудовування ДІ - область сингулярного розкладання) [17]	Стиснення з втратами, *QF*=75	0.9944	1	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0.9944	0.9944	1
	Мультиплікативний шум с *D*=0.0005	0.9888	1	1
Метод Коха і Жао (частотна область вбудовування ДИ) [14]	Стиснення з втратами, *QF*=75	0,8312	0,9864	1
	Гауссівський шум с матоочікуванням 0 і *D*=0.0005	0,7944	1	1
	Мультиплікативний шум с *D*=0.0005	1	1	1

Як видно, запропонований метод не тільки не гірший за метод [13], але й показав кращі результати в деяких випадках. Так, наприклад, при використанні стеганометоду LSB [15] в умовах стиснення з втратами з *QF*=75 значення *NC*, що відповідає максимальному об'єму ЗІ, при використані методу [13] становить 0.0864, а при використанні запропонованого методу - 0.0985, що свідчить про підвищення ефективності на 12,3%. Найбільше підвищення ефективності було досягнуто при використанні методу з кодовим управлінням вбудовування ДІ (просторова область вбудовування ДІ) [16] в умовах накладанням гауссівського та мультиплікативного шуму, що становить 51,5% та 50,8% відповідно. Якщо оцінювати ефективність методу [13] та запропонованого методу, виходячи із результатів експерименту в цілому, то середня ефективність методу [13] становить 86,975%, а методу, що був представлений у даній роботі – 99,67%.

Висновки. В роботі вирішено важливу науково-практичну задачу, що полягає у підвищенні ефективності стеганосистеми шляхом розробки модифікації методу вибору контейнера з поданої сукупності, запропонованого в [13].

В ході модифікації запропоноване поліпшення кількісної оцінки об'єму захищеної від збурення *E* інформації, що міститься у певному стеганоповідомленні, шляхом обґрунтування доцільності введення нормування об’єму відповідно до формули (11).

Проведену оцінку ефективності, зокрема порівняльну, модифікованого методу.

Отримані результати свідчать про підвищення ефективності методу вибору стеганографічного контейнера в умовах атаки проти вбудованого повідомлення, а тому і стійкості стеганосистеми в цілому, шляхом використання не абсолютного, а відносного значення об'єму захищеної інформації на 12,695%.

Список літератури

1. Torten R., Reaiche C., Boyle S. The impact of security awareness on information technology professionals' behavior. *Computers & Security*. 2018. Vol. 79. P. 68-79.
2. Alqahtani F. Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*. 2017. Vol. 124. P. 691-697
3. Mandal P.C., Mukherjee I., Goutam P., Chatterji B.N. Digital image steganography: A literature survey. *Information Sciences.* 2022. Vol. 609, P.1451-1488
4. Taher M. M., Ahmad A.R.B.HJ, Hameed R.S., Mokri S.S. A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*. 2022. Vol.100. No 5. P.1412-1427.
5. Gupta D., Gupta S., Gupta R. Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective.* 2021. Vol. 30.2. P. 63-87.
6. Abed S., Al-Roomi S. A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. *Journal on Image and Video Processing.* 2019. No. 1. https://doi.org/10.1186/s13640-019-0486-8
7. Mohammed A. M., Rossilawati S., Shukur Z., Hasan M. K. A Review on Text Steganography Techniques. *Mathematics*. 2021. No.9. 2829. URL: https://doi.org/10.3390/math9212829
8. Qi Q. A Study on Countermeasures against Steganography: an Active Warden Approach. URL: https://digitalcommons.unl.edu/ceendiss/25/
9. Selecting Cover for Image Steganography by Correlation Coefficient URL: https://ieeexplore.ieee.org/document/5459929
10. Nikishova A.V., Omelchenko T.A., Makedonskij S.A. Steganographic embedding in containersimages. *Journal of Physics: Conference Series*. 2018. Vol. 1015. No. 4. doi: 10.1088/1742- 6596/1015/4/042041
11. Kobozeva A.A., Narimanova E.V. Stegoimage disturb sensitivity estimate. *System Research and Information Technologies*. 2008. No. 3. P. 52-65.
12. Надвоцький О.Ю., Кобозєва А.А.. Метод розв'язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. URL: http://immm.op.edu.ua/files/archive/n3_v11_2021/immm_n3_v11_2021.pdf
13. Bobok I., Kobozieva A., Sokalsky S. The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message. URL: https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf
14. Fedorov A., Rubel A.S. Detection of Hidden Data Embedded by the Koch and Zhao Method. URL: https://www.researchgate.net/publication/283463767
15. Singh A.K., Singh J., Singh H.V. Steganography in Images Using LSB Technique. *International Journal of Latest Trends in Engineering and Technology*. 2015. Vol. 5, No. 1, P. 426-430.
16. Sokolov A.V. Multiple access steganographic method based on code control and frequency arrangements. *Informatics and Mathematical Methods in Simulation*. 2021. Vol. 11, No. 3, P. 147-161.
17. Melnik M.A. Steganoalgoritm, ustoichivyi k szhatiyu [A compression resistant stegano algorithm]. *Informatsiyna Bezpeka – Information Security*. 2012. No. 2. P. 99-106.
18. Images Dataset. URL: https://www.kaggle.com/datasets/pavansanagapati/images-dataset

MODIFICATION OF THE CONTAINER SELECTION METHOD TO REDUCE THE SENSITIVITY OF THE STEGANOMESSAGE TO DISTURBING INFLUENCES

S. Sokalsky

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044, Ukraine
email: sokalskiyserhiy1@gmail.com

Today, the issue of protecting information from unauthorized access is one of the key issues in the field of information technology. As digital technologies continue to spread into all areas of human activity and methods of protecting information from unwanted access are improving, the development of methods and technologies for obtaining unauthorized access to confidential information for malicious purposes does not stop either. Therefore, it is important to continue to improve information security systems, thereby hindering intruders. An integral part of any modern information security system is a steganographic system that provides a hidden data transmission channel that allows you to transmit information without revealing the fact of its existence to an attacker. The task of choosing a steganographic container allows you to solve some of the requirements for a steganographic system when building it. One of the most important requirements is to ensure the steganographic system's resistance to attacks against the embedded message, since such attacks do not require extensive knowledge of steganography and steganalysis from the attacker and do not require special technical means, which makes this type of attack simple and widespread. The aim of the work is to improve the efficiency of the steganosystem by modifying the method of selecting a container from the given set, developed by the author earlier, which will ensure the maximum possible, or at least close to the maximum, resistance of the steganomessage to attack against the embedded message for the analyzed images. This goal was achieved by modifying the quantitative assessment of the amount of protected information, namely, using the relative value of the amount of protected information to the amount of all embedded information. The result of the work is the development of a modification of the method for selecting a steganographic container, which is ready for practical application. The effectiveness of the proposed method is higher than the prototype method, and remains high regardless of which steganomethod or perturbation was used. The significance of the result is to increase the overall resistance of the steganosystem to attacks against the embedded message by using this method to select the steganocontainer.

Keywords: steganosystem, steganographic method, resistance of the steganosystem, steganographic container, digital image, singular threes.

DOI 10.15276/imms.v13.no3-4.322
УДК 004.91, 81'25, 681.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 322-334

СИСТЕМА АВТОМАТИЧНОГО КОРЕГУВАННЯ АНГЛІЙСЬКО-УКРАЇНСЬКОГО КОМП'ЮТЕРНОГО ПЕРЕКЛАДУ ДЛЯ ТЕХНІЧНИХ ТЕКСТІВ В ГАЛУЗІ АВТОМАТИЗАЦІЇ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

А.О. Стопакевич[1], А.М. Тігарєв[1], О.Р. Романюк[1], О.А. Стопакевич[2]

[1]Державний університет інтелектуальних технологій та зв'язку
1, Кузнечна, Одеса, 65029.
[2]Національний університет «Одеська Політехніка »
1, Шевченка пр. Одеса, 65044.
email: stopakevich@gmail.com

Метою роботи є розробка системи автоматичного корегування перекладених комп'ютером текстів зі специфічною термінологією, що притаманна науковим та технічним текстам в галузі автоматизації технологічних процесів. Приведений аналіз причин чому комп'ютерні перекладачі не можуть досягти високої якості англо-українського перекладу технічних текстів в зазначеній галузі. Зроблено висновок, що в межах підходу, який використовують сучасні комп'ютерні перекладачі, якість таких перекладів покращена бути не може. Проведено аналіз досвіду корегування перекладів професійними перекладачами, наявних метрик оцінки процесу та результатів корегування комп'ютерних перекладів, доступних програмних рішень для роботи з текстами, написаними українською мовою. Зроблено висновок, що для комп'ютерного англо-українського перекладу єдиним практично значимим підходом до оцінки його якості є вимірювання кількості роботи, що необхідно виконати професійному перекладачеві для того, щоб текст задовольняв літературним нормам. Аналіз наукових текстів, які були перекладені DeepL показав, що кількість такої роботи може бути істотно зменшена, оскільки помилки, які робить цей перекладач мають систематичний характер. Таким чином, аналізуючи помилки, які робить комп'ютерний перекладач, можна сформувати універсальні правила корекції для всіх перекладених певним перекладачем текстів галузі, які можуть виконуватись програмним застосунком автоматично. Ефективність підходу продемонстрована на прикладі розробки правил, що виходять з аналізу результатів перекладу двох наукових статей. Показано, що заміна приблизно 5% слів в комп'ютерному перекладі істотно підвищує його якість.

Ключові слова: корегування, комп'ютерний, переклад, автоматизація, технологічних, процесів, NLP, програма, python, термінологія, deepl.

Вступ. Українська термінологія в галузі автоматизації була сформована на базі радянської термінології, визначення якої звичайно фіксувались в державних стандартах та інших документах. Після завершення радянського періоду робота в напрямку розробки сучасної новітньої термінології в галузі автоматизації майже не ведеться. Більшість діючих ДСТУ в галузі автоматизації були введені на початку незалежності й фактично їх відмінність від радянських полягала тільки в тому, що вони були написані українською мовою. Таким чином в ДСТУ майже всі зафіксовані в радянських ГОСТ англомовні переклади термінів с залишились без змін. Проблемою цих перекладів є те, що в сучасній англійській мові приведені відповідники не застосовуються, а застосовується своя достатньо специфічна термінологія. Крім того, ця термінологія, як і галузь у цілому, постійно розвивається і коли спеціалісті стикаються з новими термінами, то без чіткої мовної термінологічної бази це призводить до утворення англійського термінологічного "суржику", розвиток якого активно спостерігається в середовищі українських IT-спеціалістів.

Наприклад, в [1] вся термінології про автоматизовані системи подається в основному за ДСТУ 2226-93. Й, хоча, українські терміни відповідають еволюції української мови з періоду незалежності, в тому числі зафіксовані в стандарті освіти за 151 спеціальністю, їх приведені англійські відповідники значною мірою не використовуються в сучасній англійській мові.

Порівняно невелика кількість наявних в інтернеті точних перекладів між текстами за галуззю автоматизації українською та англійською мовою призводить до того, що якість перекладу текстів комп'ютерними перекладачами за цією галуззю є низькою. Причин тут три. Перша причина - відносно мала кількість наявних ідентичних перекладів текстів за галуззю (особливо це стосується літератури з теорії керування). Друга причина - наявність надмірної кількості варіантів написання терміну для певного поняття (наприклад, передаточна, передатна, передавальна функція), які зафіксовані в друкованій літературі та зміна нормативного тлумачення багатозначних термінів (наприклад, управління і керування). В результаті перекладачі використовують в тексті їх всі разом, розглядаючи як синонімічні. Третя причина - різниця між традиціями створення термінів в мовах, що призводить до того, що кількість слів в англійській мові менша за українську. Наприклад, ключовим словом для автоматичного керування є дієслово to control, який суміщає два поняття, які українською мовою мають різний сенс, а саме - “контролювати” та “регулювати”. Узагальнена статистика по ряду перекладених нами текстів галузі автоматизації свідчить, що в символах тексти українською мовою займають в два рази більший обсяг, ніж їх оригінали англійською.

Приведені вище причини, що призводять до неякісного комп’ютерного перекладу, не перестануть бути актуальними в найближчий час, оскільки їх розв’язок полягає в формуванні істотної кількості якісних й термінологічно провірених перекладів, за якими зможуть навчитись коректному перекладу комп’ютерні перекладач (КП). Сучасні КП, такі як Google Translate (GT) і Microsoft Translate (MT), виникли з появи інформаційної та розрахункової можливості емпірично вивести з наявних в інтернеті джерел правила перекладу. Надалі, статистичний підхід еволюціонував до навчання нейромереж, які намагаються при підборі відповідників врахувати певний сенсовий контекст блоку тексту.

Зворотною стороною всіх технологій, що виходять з обробки емпіричного масиву даних, є відсутність гарантії якості кінцевого результату. Результат кожного запиту є непередбачуваним для розробників системи й може змінитися після наступного перенавчання. А рішення щодо застосування нових результатів навчання приймається на базі статистичних досліджень змін поведінки. Виходячи з цього, комп’ютерні перекладачі не можуть, за умов збереження поточного підходу до їх побудови, повноцінно замінити людину, особливо в терені вузькопрофільних перекладів та перекладів юридичних та фінансових документів.

Незважаючи на зазначені недоліки, КП побудовані за вказаним підходом, стали щоденним інструментом багатьох людей. Не даючи професійний переклад, вони дають, звичайно, переклад достатній для розуміння загального сенсу тексту людиною, що часто є для споживача задовільним результатом.

Поява можливості для звичайних користувачів інтернету швидко та безкоштовно отримати переклад тексту, а для бізнесу перекладати необмежену кількість документів, призвела до появи нової сфери досліджень в галузі перекладів - дослідження процесу корегування комп’ютерних перекладів (ККП, PEMT, Post-editing of machine translation output). Найважливішою практичною задачею таких досліджень є пошук шляхів скорочення часу на корегування згенерованих КП перекладів виходячи зі спостережень за діями, що виконують зі згенерованим перекладом професійні перекладачі.

В цій роботі пропонується підхід до реалізації системи автоматичного корегування текстів зі специфічною термінологією галузі автоматизації. Працездатність підходу проілюстрована за допомогою розробленого програмного застосунку, що виконує токенізацію текстових блоків та заміну їх за правилами, які формуються емпіричним чином в результаті спостереження за помилками, які припускає при перекладі КТ. Як виявляється, ці помилки мають систематичний характер, а, отже, й можуть бути систематично усунуті.

Мета роботи. Сформувати з застосуванням сучасних технологій обробки тексту новий підхід до побудови системи автоматичного корегування комп'ютерних перекладів текстів наукової та технічної літератури в галузі автоматизації. Особливістю підходу є застосування доступних безкоштовних програмних NLP технологій. Підтвердити результативність сформованого підходу шляхом розробки та дослідження роботи програмного застосунку при використанні його для корегування перекладів наукових статей.

Задачі роботи. Проаналізувати досвід корегування перекладів безкоштовно доступних комп'ютерних перекладачів професійними перекладачами, викладений в сучасній науковій літературі. Зробити висновок про те, який перекладач доцільно взяти за основу для перекладів.

1) Проаналізувати наявні метрики оцінки процесу та результатів корегування комп'ютерних перекладів, зробити висновки про доцільність їх застосування при розв'язку поставленої задачі.
2) Проаналізувати доступні програмні рішення для перевірки та корекції текстів українською мовою.
3) Сформувати підхід до побудови системи автоматичного корегування комп'ютерних перекладів технічних та наукових текстів в галузі автоматизації та запропонувати робочий варіант його програмної реалізації.
4) Дослідити потенціал застосування підходу в розробленому програмному застосунку під час розв'язку реалістичних задач комп'ютерного перекладу текстів наукових статей в галузі автоматизації.

Аналіз досвіду граматичного аналізу та корегування комп'ютерних перекладів професійними перекладачами.

Історія сучасних КП починається з 2006 р., коли Google прийняв рішення розробляти свій спеціальний перекладач - Google Translate (GT). Перша версія перекладача застосувала суто статистичний підхід й результати перекладу були гіршими, ніж у поширених тоді перекладачів, що були побудовані за класичним принципом - за правилами. В 2010 р. після кількох років роботи над проєктом, розробники перекладача досягли рівня задовільності перекладу, що став не гіршим за переклад інших розповсюджених тоді КТ, Досягши позитивного результату, Google інтегрує свій перекладач з браузером Chrome та Android.

В 2011 р. було проведено систематичне дослідження процесу перекладу з англійської на датську з застосуванням GT [2]. Групою з 8 датчан різних професійних здібностей блоки англійського тексту були перекладені як вручну, так і кореговані після застосування GT. Оцінені спеціалістами результати показали, що майже рівноймовірне, що найкращим перекладом буде або ручний або скорегований переклад. Час ручного перекладу та час корегування перекладу виявився майже однаковим. А якість кінцевого перекладу не була корельовано з часом корекції. Це пояснювалось тим, що перекладач може дати як прийнятних переклад, так й зовсім не прийнятний. Звичайно, як показують результати роботи [3] неприйнятний переклад професійні перекладачі витирають повністю й пишуть новий з чистого аркуша.

Принципове покращення GT, а згодом й інших аналогічних КП пройшло після заміни статичної технології навчання на технологію нейромереж. Приблизно

в 2016 році GT та Microsoft Translator (MT) проводять таку заміну й в них в 2017р. з'являється новий конкурент - DeepL (DL), який робить акцент на технологію глибинного навчання. В 2020 р. розробники DL презентували звіт що переклади, зроблені саме DL визнаються професійними перекладачами як найкращі в переважній кількості випадків в порівнянні з GL, ML та перекладачем Amazon. Додавання в вересні 2022 р. української мови в перелік доступним мов DL разом з більш природною та диференційованою результативною лексикою перекладу робить, на наш погляд, DL найкращим для англо-українського перекладу як технічних текстів, так й більш загальних.

В роботі [4] запропонована класифікація помилок КТ: "лексичні, синтаксичні, морфологічні, орфографічні, пунктуаційні та інші, вторинні, помилки прагматичного/культурного характеру, а також ті, що не можна чітко класифікувати за попередніми категоріями" й за цією класифікацією зроблено дослідження німецько-українського перекладу. Результати перекладу казки та публіцистичної статті далекі від ідеалу, хоча публіцистичний текст був перекладений дещо краще. Кількість помилок вимірюється десятками, при чому в них є такі, що повністю спотворюють сенс перекладу.

В роботі [5] розглянута задача англо-індонезійського перекладу анотацій наукових статей з використанням GT. Автори розділяють помилки перекладу на 13 категорій : граматичні помилки, термінологічні помилки, пропуски, синтаксичні помилки, помилки перекладу, помилки буквальності/вірності, помилки вживання, пунктуаційні помилки, помилки додавання, двозначності, помилки словоформ, помилки написання з великої літери та орфографічні помилки. В роботі продемонстрована нездатність GT зрозуміти контекст всього тексту за межами речення, що призводить до грубих помилок. Аналогічне дослідження тайського-англійського перекладу анотацій проведено в пізнішій роботі [6], в якій автори приходять до висновку що переклад GT не відповідає стандартами академічного перекладу.

Результати показового групового експерименту 2019 р. щодо дослідження феномену професійної корегування комп'ютерного перекладу з англійської на польську мову приведені в роботі [7]. Автори провели статистично достовірний експеримент з групою магістрантів - професійних перекладачів. Була розглянута задача перекладу різних текстів загальним обсягом трудомісткості перекладу приблизно в 40 хв з англійської мови на польську. Розглядався як переклад з чистого тексту, так і корекція перекладу після того, як його згенерували GT, MT та DL. Новим результатом цього дослідження, в порівнянні з експериментом з роботи [2] 2011 р., стала чітка статистична залежність економії часу відносно повістю ручного перекладу від застосовуваного КТ : економія часу з DL склала ~ 25%, MT ~ 12, GT ~ 6 %.

Нами не знайдені результати досліджень процесу корегування перекладів технічних та наукових текстів. Проблема таких досліджень в тому, що "професійний перекладач" тут не може бути розглянута як достатня групова категорія. Якщо професійний викладач не володіє певною спеціальною темою та термінологією, то зв'язок між часом перекладу з "нуля" та часом перекладу після "перекладача" буде явно складнішим, як і результат такого корегування. Нами знайдені роботи, в яких проводиться статистичний аналіз розподілення різних типів помилок в комп'ютерному перекладі, однак такі результати не дуже цікаві, оскільки істотно відрізняються в залежності від направлення переводу та стилістики тексту. Значно більший практичний інтерес має виявлення систематичності помилок, які роблять комп'ютерні перекладачі, при певному напрямку переводу в певних умовах, однак таких досліджень не знайдено.

Підсумовуючи, зробимо висновок що застосування DL для розглянутої в статті задачі є найбільш доцільним, виходячи з зафіксованих результатів експериментів, які показали, що його застосування забезпечує найбільше прискорення корегування тексту. Це забезпечується за рахунок застосування власної архітектури нейронної мережі, що здатна самонавчатись не тільки за рахунок обробки загальнодоступних точних перекладів між різними мовами, але й на основі текстів, що не мають перекладів. Основною відмінною рисою DL від GT та MT є спроба виявлення та відтворення стилістики тексту. Перекладач може враховувати не тільки жанри, але й, наприклад, діалект мови. Так, на відміну від GT, DL може відрізнити британській та американські англійські мови, а також європейську португальську й бразильську португальську. Зворотною стороною такої переваги є й недоліки - DP має найменшу в порівнянні с GT та MT кількість підтримуваних мов та найменшу швидкість перекладу.

Аналіз проблеми оцінки якості комп'ютерних перекладів та результатів їх корегування. Кількість потенційно можливих перекладів одного тексту на іншу мову є достатньо великою. Множина однакових за сенсом перекладів тим не менш не може бути прийнята як повністю еквівалентна. Певне викладення може бути більш зрозумілим, а інше - більш лаконічним, одне - звучати більш сучасно, інше - більш офіційно. КП не формують переклад, намагаючись досягти подібні цілі, тому зараз критерій якісного комп'ютерного перекладу доцільно сформулювати лише в негативній постановці - як відсутність помилок перекладу (наприклад в межах класифікації з 13 пунктів роботи I8]). Проблема визначення метрик якості переводу стискається з тим, що потрібно проводити порівняння з певним "вірним" перекладом або орієнтуватись на системи автоматичної перевірки граматики та стилю тексту. Перший підхід є цікавим для дослідження процесу перекладу та корегування перекладу при різних вхідний умовах. Такими чином, спостерігаючи за "трудовитратами" перекладачів ми робимо певні висновки. Другий підхід показує нам певні некоректності й дослідження полягає в оцінці їх серйозності та кількості необхідних замін для того, щоб досягти безпомилковий переклад.

Приведемо найбільш поширені метрики оцінювання переведеного тексту (гіпотези) відносно еталону (ручного перекладу людиною). Найбільш популярною метрикою є BLEU, яку запропонувала фірма IBM. ідея якої полягає в розрахунку точності співпадіння слів чи ланцюжків слів з еталоном з урахуванням штрафу за малу величину тексту. Проблемою цієї метрики є те, що збільшення показника не обов'язково означає покращення тексту. Наприклад, в одному реченні лише одне слово не вірне, але воно спотворює сенс усього речення. Метрика NIST - це модифікація BLEU, яка зважує слова чи ланцюжки слів за інформаційністю. Міра інформаційності слова приймається оберненою до частотності застосування слова. Обидва варіанти не підходять для оцінки перекладу словотворчими мовами, такими як українська чи словацька. Англійська мова переважно є аналітичною, це означає відсутність різниці між називним та знахідним відмінками, наявність жорстких порядків слів тощо. Українська мова переважно характеризується синтетичною морфологією. Це забезпечується численні форми та морфеми, словотворчі суфікси, що змінюють основи слів, та модифікації слів, що виражають різні граматичні категорії (наприклад, рід, число, відмінок) переважно за однією формальною ознакою. Тому для оцінки української мови доцільна лише метрика METEOR. METEOR - це модифікація BLEU, яка розглядає як еталон не фіксовану структуру, а множину структур, яка містить всі можливі синоніми та відмінки слів. Можливо також подальше ускладнення метрики шляхом застосування одночасно декількох мір точності: влучності, повноти та *F*-фактору.

Найбільш поширеними метриками, що виходять з трудовитрат є PETpT та TER. PETpT це - нормалізований до кількості символів час перекладу, a translation

Error Rate (TER) - кількість необхідних правок блоку тексту людиною для того, щоб текст став відповідним. Деякі дослідники як признак трудовитрат також розглядали тести. Ідея тут полягає в спостереженні скільки слів треба зафіксувати очима, що пов'язано теж з певною ментальною роботою. Приклади програм, які можуть бути застосовані для таких досліджень - це Translog-II [9] та PosEdiOn [10]

Виходячи зі складності формування всіх можливих вірних перекладів в українській мові, доцільно застосовувати як критерій якості машинного переводу тільки критерії витрачених на корегування трудовитрат, такі як PETpT та TER.

Аналіз доступних програмних рішень для перевірки та корекції текстів українською мовою. В першу чергу відмітимо перелік джерел awesome-ukrainian-nlp, розміщений на github Крім посилань на ключові інструменти, моделі й бібліотеки, перелік містить збірник гігабайтів оброблений й необроблених текстів українською мовою, паралельних перекладів, словників тощо. Це саме ці матеріали, які є базою всіх NLP рішень українською мовою.

Серед програмних рішень, що перевіряють орфографію текстів українською мовою та можуть запропонувати коректні виправлення, слід обов'язково відмітити систему LanguageTool. Ця система була розроблена в 2003 р. й досі набирає популярність. Система побудована класичним чином з застосуванням правил, що робить її порівняно невибагливою до ресурсів. Система безкоштовна, тому в принципі її можна інсталювати собі на сервер, а також застосовувати десктопної перевірки орфографії в десктопних версіях Office. Система перевірки української мови має більше 1000 правил, при чому система враховує всі особливості правопису 2019 р. Важливо підкреслити, що система слідкує за чистотою й сучасністю мови, тому система правил передбачає виключення т.зв. барбаризмів (суржику та інших неправильних слів та словосполучень) й застарілих термінів. В роботі [11] була концептуалізована та опробувана чорнова версія системи, яка позиціонується як потенційно альтернативне до LanguageTool рішення, базою якого є технології NLP. Показано, що система може не тільки виявляти, але й автоматично виправляти певні помилки.

У обидвох найбільш популярних NLP-бібліотеках для структурного аналізу текстів (токенізації, лематизації тощо) - Spacy і NLTK - реалізована підтримка української мови. В бібліотеці Spacy ця підтримка реалізована на високому рівні. Так, для системи Spacy регулярно оновлюються українські бази чотирьох розмірів, найбільша з яких займає обсяг на сам написання біля 400 МБ. При застосуванні NLTK позитивний результат отримати можна, але розробник може зустрітись з рядом проблем, обумовлених недостатньою підтримкою української мови, деякі з яких проілюстровані в роботі [12].

Існуючі рішення щодо морфології текстів для українською мови є зараз достатньо недосконалими. Тому такі задачі як провідміняти словосполучення, а тим паче замінити одне словосполучення на інше в тому ж відмінку й числі не мають гарантовано працюючого методу розв'язку. В роботах [11, 12] автори вказують на доступність бібліотеки pymorhpy. Однак базою цієї бібліотеки є російська мова (українська розглядається лише як експериментальна), розвиток бібліотеки припинено й ця бібліотека розв'язує свою задачу не спираючись на правила українського правопису достатньою мірою (тим паче не спирається й на норми правопису 2019 р.). Аналогічні результати й у іншої подібної, але комерційної бібліотеки - morpher.

Таким чином, підсумовуючи сказане можемо заключити, що тонізація текстів українською мовою може бути проведена на високому рівні й перевірка правопису теж. Проблемним місцем є відмінювання слів й особливо словосполучень. Повністю відсутні готові рішення, які дозволяють встановити повну відповідність між словами в українському тексті та словами в його перекладі

англійською мовою (чи навпаки). Не розв'язаною проблемою є виділення авторських позначень та введених змінних з наукових текстів будь-якою мовою. З більш докладний оглядом основних програмних лінгвістичних технологій, що можуть бути застосовані при розробці застосунків для обробки текстів українською мовою та рядом інших європейських мов рекомендуємо ознайомитись в роботі [11].

Розробка підходу до побудови системи автоматичної корекції комп'ютерних перекладів технічних та наукових текстів в галузі автоматизації. Для того, щоб сформувати підхід були проаналізовані результати отриманих за допомогою DL англо-українських перекладів ряду наукових статей, присвячених розв'язанню задач автоматизації технологічних процесів хіміко-технологічного типу. Аналіз результатів перекладу показав, що характер помилок в таких текстах має достатньо систематичний характер. Таким чином, знаючи контекст тексту, англійський текст та згенерований переклад, можливо проводити автоматичну корекцію за допомогою спеціально сконструйованої системи правил. Критерієм в такому підході буде мінімум невірних замін. Введення додаткових правил звичайно не має істотно змінювати поведінку перекладача, тому переважна кількість правил має бути точковою й обов'язково спиратися на наявність певних ключових слів в англійській версії оброблюваного речення.

Послідовність роботи користувача з системою наступна:

1) Завантаження статті (звичайно як PDF файлу)

2) Виділення текстової частини з файлу з урахуванням особливості верстки файлу (послідовний текст, двоколонна, з нерівномірними текстовими блоками.

3) Автоматична фільтрація системою текстової частини: зайвих реквізитів, підписів рисунків, формул, що записані в окремих рядках тощо.

4) Розбивка тексту на невеликі блоки. Кожен рядок тексту (блок) має містити одне чи кілька зв'язаних речень. Якщо в рядку присутній символ переносу, то цей рядок має об'єднуватись з наступним. Користувачеві повідомляється які рядки файлу треба перевірити на наявність в них цілісного блоку тексту.

5) Переклад отриманого тексту в DL. В результаті має бути отримано два текстових файли з англійський та українським текстом з повною відповідністю між рядками текстових файлів.

6) Запуск основної програми автоматичної корекції текстових файлів й відкриття звіту в браузері. В звіті відображаються запропоновані зміни.

7) У випадку виявлення під час перегляду звіту певних блоків, які вимагають корекції, проаналізувати за функціонали сторінки звіту токени проблемного текстового блоку й загальну причину помилки, додати в базу правил необхідні зміни та ввести в програму номери змінених рядків. Оновити сторінку зі звітом в браузері.

8) Повторювати п. 7. доки результат перекладу не стане задовільним.

9) Якщо отриманий текст виглядає задовільним, то рекомендується остаточно перевірити його за допомогою LanguageTool на предмет невеликих помилок.

Як мову програмування для реалізації системи виберемо Python 3.11. Програма буде мати нескладний текстовий інтерфейс, метою якого буде відпрацювання нових правил. Базовою NLP бібліотекою для програми виберемо Spacy 3. База даних правил буде зберігатись в декількох CSV файлах. Звіт буде формуватися в спеціальній папці документу як HTML файл з застосуванням бібліотеки BeautifulSoup.

Приклади формування корекційних правил та аналіз результатів, досягнутих програмою при їх застосуванні. Як приклад розглянемо створення правил за результатами аналізу перекладу двох статей [13,14]. Позначення: **НФ** - невірний

фрагмент перекладу, **ПС** - пояснення до фрагменту, **ПР** - загально сформоване правило заміни.

Основні правила, що були застосовані надані в достатній мірі для розуміння проблеми переводу та запропонованого підходу.

НФ: Closedloop block diagram → Блок-схема замкненого циклу.

ПС: Слово “loop” має перший сенс «цикл». Звичайно КП вибирає вірне слово «контур», але в цьому випадку виявилось замало слів.

ПР: Заміна «замкнений цикл» на «замкнений контур», якщо є closed ?loop”.

НФ: Steady-state error → похибка в усталеному режимі.

ПС: Постійний буквальний переклад при наявності українського відповідника.

ПР: Заміна «похибка в усталеному режимі» на «статична похибка» якщо є steady, state, error

НФ: smaller closed loop damping coefficient → менший коефіцієнт демпфування замкненого контуру.

ПС: Постійний буквальний переклад при наявності українського відповідника. Цей термін зустрічається в українській мові, але в текстах, що присвячені аналізу сигналів.

ПР: Заміна «коефіцієнт демпфування» на «коефіцієнт затухання» (варіант згасання) якщо є damping, coefficient.

НФ: Analyze the complexity of tuning a PI controller to control liquid level - Проаналізувати складність налаштування ПІ-регулятора для контролю рівня рідини.

ПС: В англійській під “control” розуміють як «контроль», так і «регулювання». В українській мові під контролем розуміється сигналізація, тому цей переклад спотворює сенс. DP іноді перекладає liquid level control як контроль рівня рідини, а іноді – як регулювання. Хоча в текстовому блоці присутній ПІ-регулятор, для DP це не стало чомусь в цьому випадку умовою зміни «контроль» на «регулювання».

ПР: Заміна «контролю рівня» на «регулювання рівня» якщо є control, liquid чи level.

НФ: The open loop system has a process transfer function gP(s) relating the controlled variable H and the manipulated variable Fout. The transfer function gL(s) relates the output variable H and the load disturbance Fin. → Розімкнута система має передатну функцію процесу gP(s), що пов'язує керовану змінну H і керовану змінну Fout. Передавальна функція gL(s) пов'язує вихідну змінну H і збурення навантаження Fin.

ПС1: DL застосовує одночасно три форми, вважаючи їх синонімічними: передатна, передавальна та передаточна функція.

ПР1: Треба замінити всі варіанти на певний один варіант, наприклад на «передаточна».

ПС2: DL спотворив сенс, переклавши “controlled variable” і “manipulated variable” як «керована змінна». Подібна помилка має систематичний характер.

ПР2: Виправлення має спиратися на те, що після “variable” йде позначення. Якщо в тексті зустрічається «керована змінна» з позначенням, то треба його виділити й перевірити наявність біля позначення в англійській версії “manipulated variable”. Тоді цю «керовану змінну» замінюємо, наприклад, на керуючий вплив.

НФ: with two tanks in series for P control (KC = 2) and PI control (KC = 5 and TI = 5 min) → у двох послідовно з'єднаних резервуарах для P-регулювання (KC = 2) і PI-регулювання (KC = 5 і TI = 5 хв).

ПС: DL використовує в текстах як «PID-регулятор», так і «ПІД-регулятор». Тут бачимо, що це про всі форми регулятора: «P-регулювання», «PI-регулювання».

ПР: При наявності «P/PI/PID control» заміняти P/PI/PID на кириличну абревіатуру.

НФ: Root locus plot → Графік кореневого локусу.

ПС: Постійний буквальний переклад при наявності українського відповідника.

ПР: Замінити «кореневий локус» на «кореневий годограф» якщо є root, locus
НФ: so the response is not oscillatory → тому відгук не є осциляторним.
ПС: Постійний буквальний переклад при наявності українського відповідника.
ПР: Замінити «осциляторний» на «коливальний» якщо є oscillatory, response.
НФ: if the plant culture requires PI level control → якщо культура рослин вимагає ПІ-регулятор рівня.
ПС: Англійське слово "plant" – це "рослина", "технологічний об'єкт керування", "технологічна установка" і "завод". Однак первинний сенс в тематиці автоматизації зустрічатись буде дуже зрідка.
ПР: Замінити "культура рослин» на «культура виробництва» якщо є plant culture.
НФ: Extractive distillation → Екстрактивна дистиляція.
ПС: DL іноді слово "distillation" перекладає як «ректифікація», а іноді як «дистиляція».
Правильний переклад – «ректифікація», оскільки майже завжди мається на увазі апарат з флегмою.
ПР: Замінити «дистиляція» на «ректифікація» якщо в distillation.
НФ: Ternary Map (Mole Basis) → Тернарна карта (кротячий базис).
ПС1: Одне зі значень англійського слова «mole» має значення «кріт».
ПР1: Замінити «кротячий базис» на «мольні одиниці» якщо є mole basis.
ПС2: Буквальний переклад з некоректним застосуванням слова «карта».
ПР2: Замінити «тернарна карта» на «трикутна діаграма» якщо є ternary map.
НФ: to handle large disturbances → для обробки великих збурень.
ПС: DL для «large disturbances» вибирає далеко не перший сенс дієслів. «Долати» - це другий сенс дієслова handle, однак DL чомусь обрав «обробки» замінити «для обробки великих збурень» на «для подолання великих збурень», якщо в оригіналі є слово "disturbance".
ПР: Замінити «для обробки великих збурень» на «для подолання великих збурень», якщо є "disturbance".
НФ: is used to set the number of stages in each column and feed locations → використовується для встановлення кількості стадій у кожній колоні та місць подачі.
ПС: В англійській мові «тарілка» ректифікаційної колони може бути перекладена як "stage", "tray" і навіть "plate". Однак "stage" – найбільш частотний варіант. Буквальний переклад його не вірний.
ПР: Замінити «стадія» на «тарілка» якщо є distillation, column.
НФ: A 1 min deadtime is included in the temperature loops -> До температурних контурів включено час очікування 1 хв.
ПС: Українським відповідником «мертвого часу» є час запізнення.
ПР: Замінити «час очікування» на «час запізнення» якщо є dead ?time.
НФ: 1 atm case with economizer; decreases in feed flowrate → Випадок з економайзером при тиску 1 атм; зменшення швидкості потоку корму.
ПС1: Буквальний переклад "flow rate" при українському відповіднику «витрата».
ПР1: Замінити «швидкість потоку» на «витрату потоку» якщо в АТ є flow ?rate.
ПС2: DL бере перше значення іменника feed й отримує "корм", що є зовсім за контекстом.
ПР2: Замінити «корм» на «живлення» якщо є feed.
НФ: An underdamped second-order system has a characteristic equation → Недодемпфована система другого порядку має характеристичне рівняння.
ПС: Буквальний переклад слова "underdamped" замість українського відповідника.
ПР: Замінити «недодемфована» на «коливальна» якщо в АТ є underdamped, system.

Сформовані правила для додавання в базу необхідно віднести до певної категорії та занести в спеціальному вигляді в відповідний до цієї категорії файл.

В першу чергу відпрацьовуються наступні пари токенів:
- amod (adjectival modifier) – прикметник + іменник
- nmod (nominal modifier) – іменник + іменник
- conj (conjunction) – сполучені слова.
- obj (object) – дієслово + об’єкт
- csubj (clausal subject) – дієслово + суб’єкт

Далі відпрацьовується заміна окремих слів на окремі слова. Наступний крок - заміна послідовностей з нефіксованою кількістю слів (в порядку починаючи з найбільшої кількості). Останній крок - заміна послідовностей, що вимагає програмного коду (на поточному етапі це виявлення змінних для того, щоб скорегувати невірний переклад “manipulated variable” як керованої змінної. Звіти програми для двох статей після досягнення рівня задовільного перекладу показані на рис. 1. і 2.

79	To illustrate this feature let us consider a single tank with the process, load, transmitter and valve transfer functions discussed above with the block diagram shown in Fig. 2. There are two clos-edloop transfer functions. The “servo” transfer function relates the response of the controlled process variable to a change in the controller setpoint. Using Aspen Dynamics labeling, the signals into the controller are the process variable signal (PV) from the transmitter and, the setpoint signal (SP).	Щоб проілюструвати цю особливість, розглянемо один резервуар з описаними вище передатними функціями процесу, навантаження, датчика і клапана, блок-схему якого показано на рис. 2. Існує дві замкнені передавальні функції. Передавальна функція "сервоприводу" пов'язує реакцію контрольованої змінної процесу на зміну уставки регулятора. Використовуючи маркування Aspen Dynamics, сигналами, що надходять до контролера, є сигнал змінної процесу (PV) від датчика та сигнал уставки (SP).	Щоб проілюструвати цю особливість, розглянемо один резервуар з описаними вище ~~передатними~~ передаточними функціями процесу, навантаження, ~~датчика~~ давача і клапана, блок-схему якого показано на рис. 2. Існує дві замкнені ~~передавальні~~ передаточні функції. ~~Передавальна~~ Передаточна функція "сервоприводу" пов'язує реакцію ~~контрольованої~~ керованої змінної процесу на зміну ~~уставки~~ завдання регулятора. Використовуючи маркування Aspen Dynamics, сигналами, що надходять до контролера, є сигнал змінної процесу (PV) від ~~датчика~~ давача та сигнал ~~уставки~~ завдання (SP).
80	The controller output signal (OP) goes to the valve in the exit line.	Вихідний сигнал контролера (OP) надходить на клапан у вихідній лінії.	Вихідний сигнал контролера (OP) надходить на клапан у вихідній лінії.
81	Using an integral time of tI = 2 min gives the root locus plot shown in Fig. 9 .	Використання інтегрального часу tI = 2 хв дає графік кореневого локусу, показаний на рис. 9.	Використання ~~інтегрального~~ часу ізодрому tI = 2 хв дає графік кореневого ~~локусу,~~ годографа, показаний на рис. 9.

Рис. 1. Фрагмент звіту програми щодо результатів корегування перекладу статті [13]

51	###3.1. Basic control structure for 10 atm case	###3.1. Базова структура управління для випадку 10 атм	3.1. Базова структура ~~управління~~ САК для випадку 10 атм
52	The well-established control structure proposed by Grassi (1992) is the basis for the design, which was used in the previous work for the high solvent flowrate case at 1 atm. Fig. 6 shows the structure in which the solvent is ratioed to the feed and both reflux ratios are controlled. Conventional PI controller are used except for level loops, which are proportional with Kc = 2. The basic control structure consists of the following loops.	Добре відома структура управління, запропонована Grassi (1992), є основою для проектування, яка була використана в попередній роботі для випадку з високою швидкістю потоку розчинника при 1 атм. На рис. 6 показано структуру, в якій співвідношення розчинника і подачі контролюється, а також обидва співвідношення рефлюксу. Використовується звичайний ПІ-регулятор, за винятком контурів рівня, які є пропорційними з Kc = 2. Базова структура управління складається з наступних контурів.	Добре відома структура ~~управління,~~ САК, запропонована Grassi (1992), є основою для ~~проектування,~~ синтезу, яка була використана в попередній роботі для випадку з високою ~~швидкістю~~ витратою потоку розчинника при 1 атм. На рис. 6 показано структуру, в якій співвідношення розчинника і подачі ~~контролюється,~~ регулюється, а також обидва ~~співвідношення рефлюксу.~~ флегмових числа. Використовується звичайний ПІ-регулятор, за винятком контурів рівня, які є пропорційними з Kc = 2. Базова структура ~~управління~~ САК складається з наступних контурів.
53	1. Feed is flow controlled. This is the throughput manipulator.	1. Подача регулюється за витратою. Це маніпулятор пропускної здатності.	1. Подача регулюється за витратою. Це маніпулятор пропускної здатності.
54	2. Solvent flow is ratioed to feed flow.	2. Потік розчинника співвідноситься з потоком подачі.	2. Потік розчинника співвідноситься з потоком подачі.
55	3. Reflux drum levels are controlled by distillate flows.	3. Рівні в зворотному барабані контролюються потоками дистиляту.	3. Рівні в ~~зворотному~~ ~~барабані~~ флегмовому баці контролюються потоками дистиляту.
56	Fig. 6. Base-case control structure using S/F, RR1 and RR2.	Рис. 6. Базова структура управління з використанням S/F, RR1 і RR2.	Рис. 6. Базова структура ~~управління~~ САК з використанням S/F, RR1 і RR2.

Рис. 2. Фрагмент звіту програми щодо результатів корегування перекладу статті [14]

Узагальнені результати по перекладу роботи [13] : з 2337 слів 97 слів було додано й 102 слова видалено. Узагальнені результати по перекладу роботи [14]: з 2300 слів 138 слів було видалено й 147 слів додано. Таким чином, для корекції тексту необхідно змінити приблизно 5% від його слів.

Висновки

1. Результати автоматичного перекладу текстів наукових статей галузі автоматизації технологічних процесів з англійської на українську з використанням DeepL показують, що в цілому спеціаліста є зрозумілим про що йде мова в оригінальному тексті.
2. Тим не менш, переклад є далеким від літературно прийнятного. Замість прийнятих в українській термінології галузі У цілому помилки, які робить КТ є легко помітними (на кшталт “культура рослин” замість культури виробництва чи “корм колони” замість “живлення колони). Однак, зустрілась й така, яка паплюжить смисл, але є непомітно, коли як вхідна, так і вихідна змінна об’єкту в системі позначень стали “керованими змінними”.
3. У цілому помилки, які робить КТ є легко помітними (на кшталт “культура рослин” замість культури виробництва чи “корм колони” замість “живлення колони). Однак, зустрілась й така, яка паплюжить смисл, але є непомітно, коли як вхідна, так і вихідна змінна об’єкту в системі позначень стали “керованими змінними”.
4. Помилки та неточності, які припускає КТ мають систематичний характер. Застосування запропонованого підходу до корегування тексту дозволяє істотно компенсувати фактор систематичних помилок, таким чином час очікуваного редагування тексту, який пройшов комп’ютерний перекладач та запропонований коректор буде істотно меншим ніж час редагування тексту, який піддався тільки комп’ютерному перекладу.
5. Статистичний аналіз показує, що в розглянутих перекладах достатньо замінити лише 5% слів для того, щоб істотно покращити літературний рівень тексту.

Список літератури

1. Нікітін О.К., Зайцев В.М., Толочко Т.О. Приладобудування та автоматизація. Терміни і визначення. Київ : КПІ ім. Ігоря Сікорського, 2019. Ч. 1. 202 с.
2. Michael C., Dragsted B., Elming J. The process of post-editing: A pilot study. *Proceedings of the 8th International NLPCS Workshop*. Denmark, Samfundsliterattur: Copenhagen Business School. P. 131-142.
3. Parra Escartín C., Arcedillo M. A fuzzier approach to machine translation evaluation: A pilot study on post-editing productivity and automated metrics in commercial settings. *Proceedings of the Fourth Workshop on Hybrid Approaches to Translation (HyTra)*, Beijing. Stroudsburg, PA, USA, 2015. P. 40–45. URL: https://doi.org/10.18653/v1/w15-4107.
4. Моісєєва Н., Дзикович О., Штанько А. Машинний переклад: порівняння результатів та аналіз помилок DeepL та Google Translate. *Advanced Linguistics*. 2023. № 11. С.78-82. https://doi.org/10.20535/2617-5339.2023.11.27759
5. Ismail A., Hartono R. Errors Made in Google Translate in the Indonesian to English Translations of News Item Texts. *ELT Forum: Journal of English Language Teaching*. 2016. Vol. 5, no. 2. Article 2. URL: https://journal.unnes.ac.id/sju/index.php/elt/article/view/11228.
6. Tongpoon-Patanasorn A., Griffith K. Google Translate and Translation Quality: A Case of Translating Academic Abstracts from Thai to English. *PASAA: Journal of Language Teaching and Learning in Thailand*. 2020. No. 60. P. 134–163.
7. Kur M. Method of measuring the effort related to post-editing machine translated outputs produced in the English>Polish language pair by Google, Microsoft and

DeepL MT engines: A pilot study. *Beyond Philology An International Journal of Linguistics, Literary Studies and English Language Teaching*. 2019. No. 16/4. P. 69–99. URL: https://doi.org/10.26881/bp.2019.4.03

8. Ismail A., Hartono R. Errors Made In Google Translate In The Indonesian To English Translations Of News Item Texts. *Journal of English Language Teaching*. 2016. Vol. 5. URL: https://api.semanticscholar.org/CorpusID:58690342.
9. Giraldo Ospina D. L., Naranjo Ruiz M., Romero Ramírez L. C. A methodological proposal integrating the translation process into the study of cognitive effort. *Cadernos de Tradução*. 2022. Vol. 42, no. 1. P. 1–24. URL: https://doi.org/10.5007/2175-7968.2022.e84845
10. Oliver A., Alvarez S., Badia T. PosEdiOn: Post-Editing Assessment in PythOn. *Proceedings of the 22nd Annual Conference of the European Association for Machine Translation*, Lisboa, 1 November 2020. P. 403–410. URL: https://aclanthology.org/2020.eamt-1.43.pdf
11. Холодна Н., Висоцька В. Технологія виправлення граматичних помилок в україномовному текстовому контенті на основі методів машинного навчання. *Радіоелектроніка, інформатика, управління*. 2023. № 1. С. 114–140. URL: https://doi.org/10.15588/1607-3274-2023-1-12
12. Tmienova N., Sus B. System of Intellectual Ukrainian Language Processing. *Information Technologies and Security* 2019. P. 199–209. URL: https://ceur-ws.org/Vol-2577/paper16.pdf.
13. Luyben W. L. Liquid level control: Simplicity and complexity. *Journal of Process Control*. 2020. Vol. 86. P. 57–64. URL: https://doi.org/10.1016/j.jprocont.2019.12.008
14. Luyben W. L. Control of heat-integrated extractive distillation processes. *Computers & Chemical Engineering*. 2018. Vol. 111. P. 267–277. URL: https://doi.org/10.1016/j.compchemeng.2017.12.008

А.О. Стопакевич, А.М. Тігарєв, О.Р. Романюк, О.А. Стопакевич

AUTOMATIC CORRECTION SYSTEM OF ENGLISH-UKRAINIAN COMPUTER TRANSLATION FOR TECHNICAL TEXTS IN THE FIELD OF AUTOMATION OF TECHNOLOGICAL PROCESSES

A.O. Stopakevych[1], A.M. Tigarev[1], O.R. Romanyuk[1], O.A. Stopakevych[2]

[1]State University of Intellectual Technologies and Telecommunications
1, Kuznechna, Odesa, 65029, Ukraine
[2]National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
email: stopakevich@gmail.com

The purpose of the work is to develop a system of automatic correction of computer-translated texts with specific terminology, which is inherent in scientific and technical texts in the field of automation of technological processes. An analysis of the reasons why computer translators cannot achieve high-quality English-Ukrainian translation of technical texts in the specified field is given. It was concluded that within the limits of the approach used by modern computer translators, the quality of such translations cannot be improved. An analysis of the experience of translation correction by professional translators, available metrics for evaluating the process and results of correction of computer translations, and available software solutions for working with texts written in the Ukrainian language was carried out. It was concluded that for computer English-Ukrainian translation, the only practically significant approach to assessing its quality is measuring the amount of work that must be performed by a professional translator in order for the text to meet literary standards. The analysis of scientific texts that were translated by DeepL showed that the amount of such work can be significantly reduced, since the errors made by this translator are systematic. Thus, by analyzing the mistakes made by a computer translator, it is possible to form universal correction rules for all texts translated by a certain translator of the industry, which can be performed automatically by the software application. The effectiveness of the approach is demonstrated on the example of the development of rules resulting from the analysis of the results of the translation of two scientific articles. It is shown that replacing approximately 5% of words in computer translation significantly increases its quality.

Keywords: correction, computer, translation, automation, technological, processes, NLP, program, python, terminology, deepl.

DOI 10.15276/imms.v13.no3-4.335
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 335-341

ВИЯВЛЕННЯ МАСШТАБУВАННЯ З КОЕФІЦІЄНТОМ, МЕНШИМ ОДИНИЦІ, ЯК ФАЛЬСИФІКАЦІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, Є.В. Тимофеєв, О.Ю. Лебедєва

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: v.v.zorilo@op.edu.ua

Виявленню підробок цифрових зображень у відкритих джерелах присвячено багато уваги. Це пов'язано із поширенням мобільної фото- і відео-техніки, з доступністю та багатофункціональністю графічних редакторів, а також із зростанням кіберзлочинності. Кібербезпека та/або інформаційна безпека мають за мету в тому числі і забезпечення цілісності цифрових зображень. Порушення цілісності цифрових зображень можна виконати багатьма методами: клонування, фотомонтаж, масштабування (збільшення або зменшення об'єкта) тощо. Виявленню масштабування присвячено ряд робіт, однак часто запропоновані рішення виявляються мало ефективними при масштабуванні-зменшенні або масштабуванні з коефіцієнтом, меншим одиниці. Мета даної роботи – виявлення масштабування цифрового зображення шляхом розробки метода, заснованого на аналізі високочастотних компонентів дискретного косинусного перетворення. Експериментально встановлено, що при зменшенні частини зображення високочастотні коефіцієнти дискретного косинусного перетворення збільшуються. Вдалося встановити порогове значення, що дозволило відділити зменшені частини цифрового зображення від оригінальних. На основі проведених досліджень розроблено метод виявлення масштабування, ефективність якого в термінах помилок 1 і 2 роду становить 7% і 14% відповідно. Розроблений метод є ефективним при зменшенні об'єктів не менш ніж втричі, а також при високій контрастності зменшуваних об'єктів. При зменшенні частини зображення вдвічі кількість помилок 1 роду зростає до 30%. Предметом подальших досліджень авторів є зменшення обмежень розробленого методу.

Ключові слова: масштабування, цифрове зображення, виявлення фото підробок, дискретне косинусне перетворення.

Вступ. Цифрові зображення часто піддаються обробці, або фальсифікації, і під час фальсифікації використовуються різні інструменти, в тому числі і масштабування.

Наразі вже існують різні методи для виявлення масштабування у цифрових зображеннях, проте вони мають певні обмеження [1-3]. Більшість методів виявляють масштабування у вигляді збільшення, в той час як виявлення зменшених частин, як правило, не вдається реалізувати існуючими методами, тому виявлення масштабування шляхом зменшення, або масштабування з коефіцієнтом, меншим одиниці, є актуальним питанням.

Масштабування зображення – це процес зміни розмірів цифрового зображення, який може включати в себе як збільшення (масштабування з коефіцієнтом більше 1), так і зменшення (масштабування з коефіцієнтом менше 1) його фізичних розмірів (або кількості пікселів), що впливає на його вид і якість.

Масштабування дозволяє адаптувати зображення до різних потреб і розмірів екранів, але також може використовуватись для обману або маніпуляції з цифровими зображеннями для неправильного представлення їх вмісту.

Мета роботи – виявлення масштабування цифрового зображення шляхом розробки метода, заснованого на аналізі високочастотних компонентів дискретного косинусного перетворення.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Дослідити проблематику ідентифікації порушень цілісності цифрових зображень.

2. Оцінити, як масштабування впливає на характеристики та атрибути матриці цифрового зображення.

3. Розробити та програмно реалізувати метод виявлення масштабування з коефіцієнтом, меншим одиниці.

4. Оцінити ефективність і визначити обмеження розробленого методу.

Матеріали та методи. Зображення як сигнал складається з частот різного діапазону. Фоновим областям зображення відповідають головним чином низькі частоти, контурам різного ступеня контрастності відповідають головним чином середні і високі частоти.

Логічно припустити, що при зменшенні частини цифрового зображення збільшиться різниця між значеннями пікселів зменшуваної області. Якщо це так, то мають збільшитись високочастотні коефіцієнти ДКП в відповідних блоках матриці.

Обчислимо дискретне косинусне перетворення для 8×8-блоків обраної області матриці зображення (рис.1).

	1	2	3	4	5	6	7	8
1	576.7500	-221.4898	146.0283	-90.0186	40.7500	-15.1420	4.9978	-0.1347
2	-102.5911	162.4174	-100.6773	44.8774	-6.5681	-12.7274	13.3994	-5.9939
3	-3.1311	8.2400	-32.6044	47.6053	-44.1237	34.6854	-15.7730	1.2795
4	2.1149	-28.1613	24.9271	-19.0795	10.8731	1.1795	-13.7846	14.8166
5	13.2500	-10.0994	12.5629	-13.1780	18.7500	-25.8920	25.1033	-15.0524
6	-0.1971	2.7710	1.0964	-1.3708	1.7588	-3.1728	2.9017	-1.3372
7	-1.6796	-7.2074	6.2270	5.1210	-5.2654	-3.8878	3.1044	4.4537
8	-3.7477	6.4558	-4.1849	4.9033	-0.2069	-4.7102	0.1280	4.8349

Рис. 1. Матриця коефіцієнтів ДКП

Проаналізуємо збурення високочастотних коефіцієнтів. Усього високочастотних коефіцієнтів ДКП в блоці 8×8 буде дев’ять. Вони знаходяться у правому нижньому куті матриці ДКП .

Знайдемо середнє арифметичне значення для відповідних коефіцієнтів по всім блокам, що аналізуються. Отримаємо вектор з дев’яти значень для аналізованої області.

Не існує значущої різниці, яку колірну компоненту аналізувати в даному випадку, оскільки для кожної матриці R, G, B результати не будуть принципово відрізнятися.

Сформуємо базу з 200 зображень для проведення експерименту, які було взято на сайті Open Images Dataset, що є одним з загальноприйнятих для проведення експериментів з зображеннями [4].

Зображення відрізняються за розміром, при цьому всі вони збережені у форматі з втратами (JPEG) та мають коефіцієнт якості (Approx. quality factor) не менше 70%. Проведення масштабування-зменшення виконано за допомогою програми Adobe Photoshop 2022 наступним способом.

1. Під час завантаження ЦЗ встановити опцію профілю кольорів «Без змін» для збереження оригінальних кольорових налаштувань.

2. За допомогою інструмента «Виділення об'єктів» виділити потрібний об'єкт на зображенні для подальшого зменшення (рис. 2).

3. Створити копію об'єкта на новому шарі, використовуючи праву клавішу миші і опцію «Скопіювати на новий шар» (рис. 3).

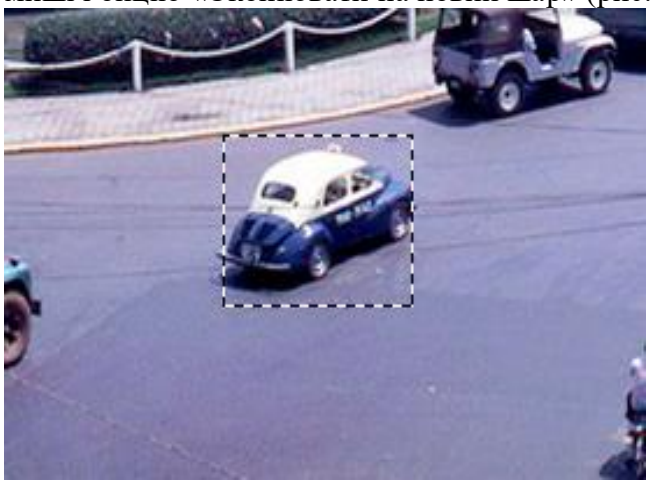


Рис. 2. Приклад виділення області для масштабування

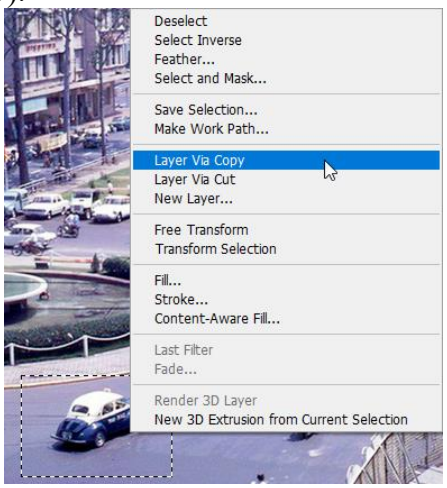


Рис. 3. Копіювання обраної області на новий шар

4. Повторно виділити вже скопійований об'єкт на основному зображенні.

5. Виконати заливку обраної області, користуючись опцією «Виконати заливку» у контекстному меню. Налаштування заливки включають в себе зміст (враховуючи зміст) та режим накладання (нормальний) (рис. 4).

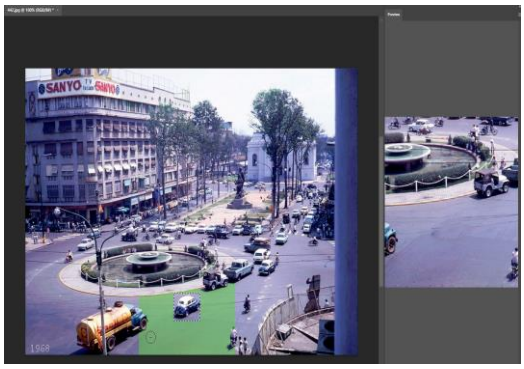


Рис. 4. Заливка області з врахуванням змісту

Рис. 5. Масштабування області за допомогою трансформації

Обрати шар з копією об'єкта та виконати масштабування за допомогою трансформації. Розмір об'єкта зменшуємо до 30%. Обраний графічний редактор дозволяє вибрати спосіб інтерполяції (бікубічна, білінійна тощо), як показано на рис. 5. Однак при проведенні обчислювального експерименту встановлено, що вид інтерполяції не впливає суттєво на результати.

6. Зберегти отримане зображення у форматі без втрат

Пункти 4-5 є критичними, оскільки для забезпечення стійкості візуального сприйняття масштабованого об'єкта на фоні оригінального зображення необхідно зробити виділену область подібною до фону на початковому зображенні. Інструмент «заливка» допомагає досягти цього ефекту. Параметри заливки можуть бути налаштовані вручну. В даній роботі проведено заливку з урахуванням змісту. Також необхідно звернути увагу на пункт 6, бо об'єкти у всіх зображеннях зменшуються саме до 30% (у 3.3 рази). Приклад зображення до та після обробки можна побачити на рис.6 та рис.7. На рис. 7 видно зменшення першої зліва мозаїки в 3 рази відносно оригіналу. Якщо не мати оригіналу, то практично неможливо візуально виявити фальсифікацію.

Результати та обговорення. Проаналізувавши 200 зображень з масштабуванням з коефіцієнтом, меншим одиниці, та без нього, можна побачити, що високочастотні коефіцієнти ДКП в блоках збільшуються по модулю. Типові результати можна побачити на рис. 8, 9, 10. Синім кольором позначений графік середнього значення високочастотних коефіцієнтів оригінального зображення, а червоним – зменшеної області зображення.

Рис. 6. Оригінальне зображення

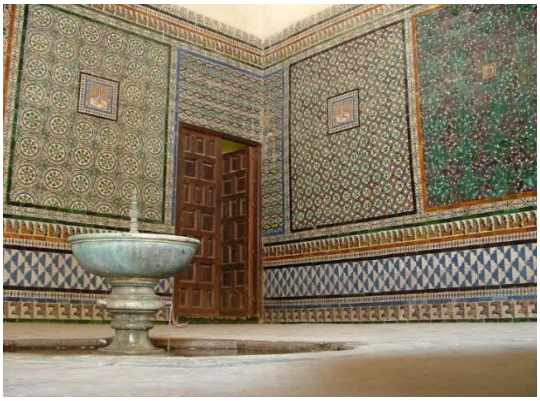


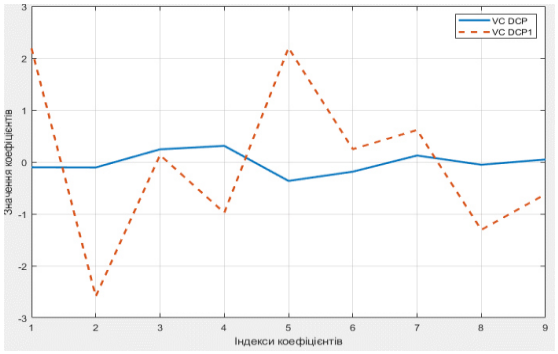
Рис. 7. Зображення з від`ємним масштабуванням

Експериментально встановлено, що для більшості зображень виділена область до масштабування мала високочастотні коефіцієнти по модулю менше двох, після масштабування – більше двох. На основі отриманих результатів розроблено метод виявлення масштабування з коефіцієнтом, меншим одиниці, заснований на аналізі високочастотних коефіцієнтів ДКП. Основні кроки даного методу наступні.

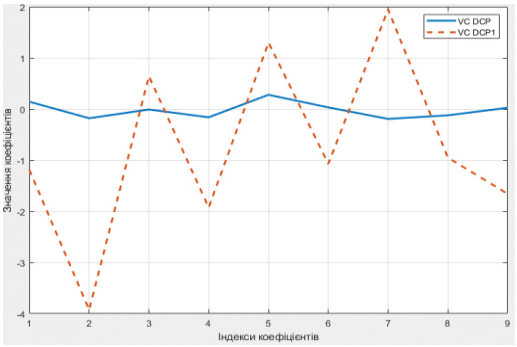
Нехай F – $m \times n$-матриця цифрового зображення. Крок 1. Виділити в матриці F область, підозрювану на наявність масштабування. Крок 2. Обрізати, при необхідності, виділену область до розмірів кратних 8. Крок 3. Для виділеної області виконати розбиття стандартним чином на блоки 8×8. Крок 4. Для кожного блоку побудувати ДКП. Крок 5. Виділити для кожного блоку серед коефіцієнтів ДКП тільки високочастотні. Крок 6. Знайти середні значення для кожного з дев'яти високочастотних коефіцієнтів ДКП в блоках, що знаходяться на відповідних місцях. Крок 7. Знайти найбільше по модулю значення серед отриманих на попередньому кроці усереднених коефіцієнтів ДКП – d_{max}. Крок 8. Порівняти найбільше значення з встановленим пороговим значенням «2»: *якщо* $d_{max}>2$ – область містить від'ємне масштабування, *інакше* – не містить.

При встановленні даного порогового значення кількість помилок 1 роду складала 7%, другого роду 14%.

Також було проведено дослідження зі зменшенням вдвічі. При пороговому значенні 2 кількість помилок 1 роду зростає до 30%. Отже, метод є ефективнішим при масштабуванні з коефіцієнтом «0.3» і менше. Також було виявлено, що метод краще працює з об'єктами високої контрастності, ніж низької. Наприклад, на рис.11 можна побачити 2 медузи: ліворуч – медуза з низькою контрастністю, праворуч – з більш високою. При зменшенні лівої медузи, середні значення високочастотних коефіцієнтів ДКП не будуть суттєво збільшуватися через низьку контрастність, коли при зменшенні правої медузи (рис.12), можна побачити тенденцію збільшення середніх значень високочастотних коефіцієнтів ДКП (рис.13).



а



а

б

б

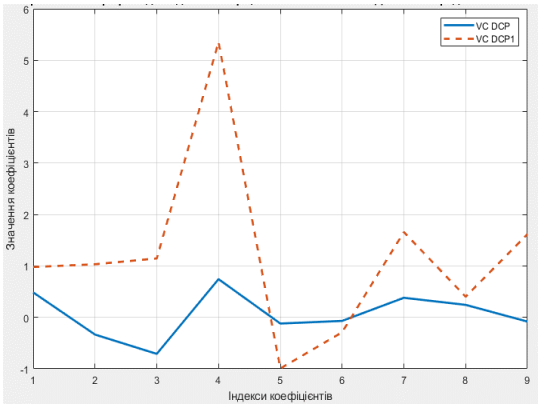
в

в

Рис. 8. Аналіз зображення №1

Рис. 9. Аналіз зображення №2

а – порівняльний графік усереднених коефіцієнтів високих частот ДКП до (синій колір) та після (червоний колір) масштабування; б – оригінальне ЦЗ; в – фальсифіковане ЦЗ



а

Рис. 11. Оригінальне зображення медуз

б

Рис. 12. Зображення зі зменшеною правою медузою

в

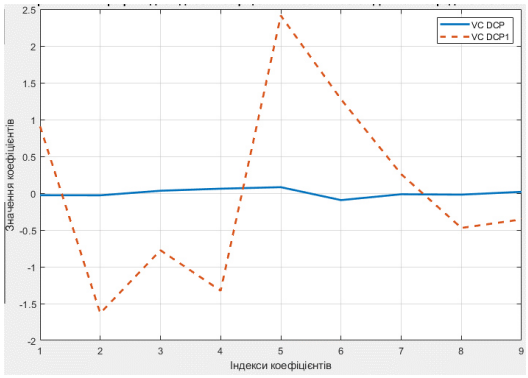


Рис. 10. Аналіз зображення №3: а – порівняльний графік усереднених коефіцієнтів високих частот ДКП до (синій колір) та після (червоний колір) масштабування; б – оригінальне ЦЗ; в – фальсифіковане ЦЗ

Рис. 13. Порівняльний графік середнього значення коефіцієнтів високих частот ДКП для зображення з медузами до та після фальсифікації

Проведені експерименти дозволили виявити обмеження розробленого методу. Дані обмеження є предметом подальших досліджень авторів статті.

Висновки. Проведено аналіз статей, присвячених виявленню масштабування як фальсифікації цифрового зображення. Встановлено, що масштабуванню з коефіцієнтом, меншим одиниці, присвячено мало уваги.

Проведено аналіз впливу масштабування з коефіцієнтом, меншим одиниці, на високочастотні коефіцієнти ДКП 8×8-блоків матриці цифрового зображення.

Результати дослідження показали, що шляхом аналізу високочастотних коефіцієнтів обраної зони цифрового зображення можна ефективно відрізнити модифіковані частини зображення від оригінальних.

За підсумками одержаних результатів був створений метод виявлення масштабування з коефіцієнтом, меншим одиниці, заснований на аналізі високочастотних компонентів ДКП блоків матриці цифрового зображення.

Ефективність розробленого методу в термінах помилок 1 і 2 роду становить 7% і 14% відповідно.

Список літератури

1. Трифонова К.О., Кілін О. Є.. Метод локалізації та ідентифікації контекстно-залежного масштабування в цифровому зображенні. URL: http://www.tkea.com.ua/siet/archive/2014-t1/117.pdf
2. Гулич В.В. Зоріло В.В., Лебедєва О.Ю. Виявлення частин цифрового зображення, зменшених після фальсифікації. *Інформатика та математичні методи в моделюванні.* 2022. Том 12. № 1-2. С.46-53.
3. Берія Д.Ю., Войтовецька М.Є., Козаченко Н.Г., Зоріло В.В., Лебедєва О.Ю. Виявлення порушень цілісності цифрових зображень в контексті цифрової криміналістики. *Інформатика та математичні методи в моделюванні*. 2021.Т.11. №3. С. 190-199.
4. Open Images Dataset V7. URL: https://storage.googleapis.com/openimages/web/visualizer/index.html

DEVELOPMENT OF THE DIGITAL IMAGE SCALING DETECTION METHOD

V.V. Zorilo, E.V. Timofeiev, O.Y. Lebedieva

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: v.v.zorilo@op.edu.ua

Detection of digital image forgeries in open sources has garnered significant attention. This is attributed to the proliferation of mobile photo and video technology, the accessibility and multifunctionality of graphic editors, as well as the rise in cybercrime. Cybersecurity and/or information security aim, among other things, to ensure the integrity of digital images. Violations of the integrity of digital images can be carried out through various methods such as cloning, photo manipulation, scaling (enlarging or reducing objects), etc. Scaling detection has been the subject of several works, but often the proposed solutions prove to be ineffective for scaling down or scaling with a coefficient less than one. The goal of this work is to detect scaling of digital images by developing a method based on the analysis of high-frequency components of discrete cosine transformation. Experimental findings indicate that when a portion of the image is reduced, the high-frequency coefficients of the discrete cosine transformation increase. A threshold value was successfully established, allowing the separation of scaled portions of the digital image from the original ones. Based on the conducted research, a scaling detection method was developed, with an error rate of 7% and 14% for types 1 and 2 errors, respectively. The developed method proves effective for scaling objects by at least threefold and high-contrast scaled objects. However, when reducing a portion of the image by half, the error rate for type 1 errors increases to 30%. Further research by the authors aims to reduce the limitations of the developed method.

Keywords: scaling, digital imaging, photo detection, discrete cosine transformation.

DOI 10.15276/imms.v13.no3-4.342
УДК 621.317

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 342-348

ВАРІАНТ СИСТЕМИ ВИЗНАЧЕННЯ ТЕХНІЧНОГО СТАНУ ЦИФРОВИХ ОБ'ЄКТІВ

В.О. Хорошко, В.В. Кузавков, Ю.В. Болотюк

Військовий інститути телекомунікацій та інформатизації імені Героїв Крут
45/1, Князів Острозьких, Київ, 01011, Україна
e-mails: professor_va@ukr.net; nevse@ukr.net; yuliia.bolotiuk@viti.edu.ua

Широке залучення цифрових пристроїв (систем) в людській діяльності висуває актуальне питання забезпечення надійності функціонування подібних систем. В свою чергу, забезпечення надійності не можливо без ефективної системи контролю та діагностування технічного стану обраного об'єкту контролю. З іншого боку, виробник цифрового обладнання не зацікавлений у безвідмовному багаторічному функціонуванні виготовлених ним зразків, оскільки це сповільнює виробничий цикл та відповідно зменшує прибутки. Задача контролю за технічним станом будь якого цифрового пристрою покладається цілком на користувача зазначених засобів. Відомо, що у протистоянні окремих засобів контролю та уніфікованих систем контролю цифрового устаткування перемагають уніфіковані системи контролю на базі безконтактних методів реєстрації діагностичної інформації. Структура таких систем також відома, це комп'ютерна вимірювальна система зі спеціалізованим програмним забезпеченням збору та обробки діагностичної інформації, а також інтелектуальної системи підтримки прийняття рішення. Запропоновані авторами рішення базуються на безконтактному індукційному методі діагностування та уніфікованому діагностичному параметрі який відображує фізико-хімічні процеси старіння напівпровідникових структур цифрових радіоелектронних компонентів. Розглядається застосування математичних методів для побудови системи технічного діагностування цифрових об'єктів. Представлено узагальнену методику контролю цифрового обладнання шляхом побудови перевірних тестових послідовностей. В основу методики покладено сучасні методи отримання та обробки діагностичної інформації, алгоритми побудови діагностичних тестів. Отримані результати дають можливість автоматизувати процес визначення фактичного технічного стану сучасного цифрового обладнання.

Ключові слова: діагностичний параметр, модель, тест, алгоритм.

Вступ. До складу сучасних систем обробки та передачі інформації, окрім цифрових елементів входять і аналогові (особливо в складі блоків перетворення для передачі по фізичним каналам). В окремих системах, проведення контролю покладається на вбудовані системи, функціонал яких дуже обмежено. Проведення якісного діагностування можливо лише із залученням спеціальних програмно-апаратних засобів [1, 2].

Певну складність в практичній реалізації уніфікованої автономної автоматизованої системи контролю (діагностування) (ААСД) викликає процес створення діагностичних паспортів РЕО (бази еталонних зразків діагностичного параметру, якій виміряно під час проведення перевірки).Створення такого паспорту вимагає або тісної співпраці з виробником радіоелектронного обладнання (РЕО) або досконалого розуміння структури та алгоритмів функціонування об'єкту контролю з можливостю проведення чисельних, статистично обґрунтованих випробувань.

Отже, перевірка цифрових систем необхідна для забезпечення надійності та безвідмовності функціонування об'єкту контролю. Відомо декілька методів перевірки цифрових систем:

- функціональне тестування: включає запуск системи з різними вхідними даними та перевірку, чи видає вона очікувані результати;
- тестування кордонних значень: перевірка реакції системи на межові значення вхідних даних;
- тестування на випадкових даних: використання випадкових даних для перевірки системи на непередбачувані ситуації;
- тестування згідно зі специфікаціями: порівняння результатів системи з тими, які вказані в технічних специфікаціях;
- тестування на виключні ситуації: створення умов, які викликають помилки або некоректну роботу системи.

Один з варіантів перевірки цифрових систем це перевірка на безперервність. Перевірка на безперервність, яка містить в собі:

- тестування відмов: симуляція різних типів відмов (програмні, апаратні) та перевірку, чи може система коректна відновитися;
- дублювання: використання дубльованих або зайвих компонентів для забезпечення роботи системи навіть після відмови одного з компонентів;
- запобігання відмовам: використання методів для попередження відмов, таких як контроль справжнього часу, моніторинг стану апаратного забезпечення тощо;
- резервне копіювання: створення резервних копій даних для відновлення в разі втрати;
- моніторинг: встановлення систем моніторингу для відстеження проблем та аномалій у реальному часі;
- заплановане обслуговування: регулярне технічне обслуговування та оновлення системи для запобігання відмовам через знос.

У системах критичної інфраструктури іноді застосовуються комплексні підходи до перевірки, які поєднують кілька методів для забезпечення найвищої надійності. Ці методи можна комбінувати та налаштовувати залежно від конкретних потреб і характеристик ОК.

Суперечливість вимог при складанні тестових послідовностей для контролю та діагностики безперервності цифрових систем (ЦС) проявляється у наступному:

- необхідно забезпечити синтез тестів за практично прийнятний час;
- обрані методи синтезу тестів повинні забезпечувати повну перевірку ЦС.

Крім того, алгоритми та програми синтезу тестів повинні бути наочними та доступними для огляду, а тестові послідовності необхідно представляти у формі, зручній для налагодження програм для їх перевірки в реальних умовах експлуатації технічних засобів.

Можливість швидкого вирішення зазначених протиріч разом із розвитком цифрової техніки, на жаль, не покращується, а навпаки, знижується. Такий стан пояснюється насамперед тим, що ЦС, які підлягають контролю, значно ускладняються як структурно так і функціонально. Це ускладнення обумовлено зростанням ступеню інтеграція мікросхем, і кількості мікросхем великої та середньої інтеграції.

Робота присвячена пошуку компромісу вирішенні завдання з контролю та діагностики ЦС. З робіт [3,4,5] відомо, що достатніми умовами контрольованості мереж зв'язку є доступність функціональних елементів через первинні входи та можливість транспортування несправності до первинних виходів ЦС. У зв'язку з цим, перед початком синтезу тестових повідомлень, доцільно проаналізувати структуру ЦС для визначення ступеню його контрольованості та діагностики із заданою глибиною.

Мета статті та постановка задачі. Стрімкий розвиток мікроелектроніки та інформаційних технологій потребує від конструкторів і виробників сучасних

автономних автоматизованих систем технічного діагностування (АА СТД) розробки нових методів отримання та обробки діагностичної інформації для визначення технічного стану та локалізації несправного радіоелектронного компонента аналогових і цифрових блоків [6]. Автономна автоматизована система технічного діагностування блоків радіо електронного обладнання (РЕО) є складовою частиною системи технічного діагностування і представляє сукупність засобів, об'єкта діагностування та виконавців, які необхідні для проведення діагностування за правилами, встановленими технічною документацією. Системи технічного діагностування повинні розроблятися на стадії проектування, забезпечуватися на стадії виробництва і підтримуватися на стадії експлуатації об'єктів РЕО. Однак ці вимоги далеко не завжди виконуються. Аналіз існуючих систем технічного діагностування показав, що це обумовлено рядом суттєвих недоліків, які властиві існуючим АА СТД. Тому автономні автоматизовані системи технічного діагностування блоків РЕО, що побудовані на основі існуючих методів й методик, є малоефективними, та не відповідають сучасним вимогам.

Тому при експлуатації існуючих та створені нових перспективних об'єктів РЕО достатньо чітко визначились наступні протиріччя:

між реальними технічними можливостями об'єктів РЕО та низьким рівнем їх реалізації через низький рівень АА СТД;

між рівнем вимог, які пред'являються до АА СТД і неможливості їх задовольнити існуючим методологічним апаратом отримання, обробки та управління діагностичною інформацією;

між обмеженою ціною АА СТД та високими вимогами до її технічних характеристик.

Таким чином, основне протиріччя існуючої системи технічного діагностування блоків РЕО визначається принциповою можливістю побудови високоефективних автономних автоматизованих систем технічного діагностування на основі використання передових досягнень в області інформаційних технологій при отриманні та обробці діагностичної інформації. А також недостатньою ефективністю автоматизованих систем технічного діагностування в існуючих об'єктах РЕО, що не забезпечує локалізацію несправності з точністю до радіоелектронного компонента (РЕК).

Це протиріччя обумовлено наведеними недоліками існуючої системи технічного діагностування, яка не забезпечує локалізацію несправності з точністю до радіоелектронного компонента. Як наслідок, це призвело до створення й функціонування на сучасному етапі експлуатації об'єктів РЕО складної, не економічної, багатоконтурної системи технічного обслуговування і ремонту, що обумовлює втрату часу на контроль технічного стану й локалізацію можливих несправностей в блоках РЕО.

Для усунення даного протиріччя необхідно використовувати інформаційні технології при побудові й впровадженні автономних автоматизованих систем технічного діагностування радіоелектронних блоків на основі отримання та обробки діагностичної інформації.

Зазначене діалектичне протиріччя визначило актуальну наукову проблему, що полягає в розробленні інформаційних технологій для побудови і впровадження автономних автоматизованих систем технічного діагностування блоків РЕО на основі отримання та обробки діагностичної інформації. Проведені наукові дослідження в області застосування інформаційних технологій при діагностуванні аналогових і цифрових радіоелектронних блоків дозволили розробити нові методи отримання (динамічний, енергодинамічний, електромагнітний, індукційний та метод власного випромінювання) та обробки

діагностичної інформації [6, 7]. В статті вирішується наукове завдання розробки узагальненої методики діагностування автономною автоматизованою системою технічного діагностування блоків РЕО, що побудована на основі даних методів.

Основна частина. Загальна схема процесу підготовки та здійснення контрольно-діагностичних операцій наведена на рисунку 1.

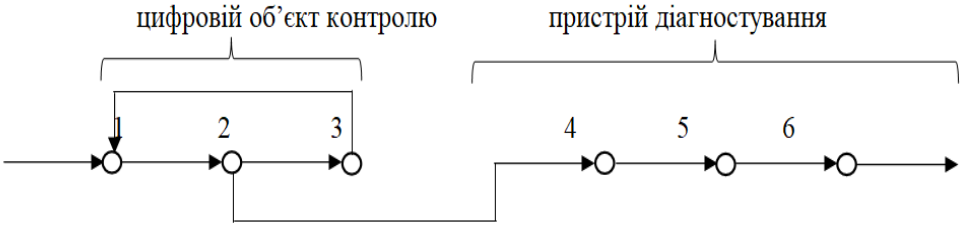


Рис.1. Етапи процесу підготовки та здійснення контрольно-діагностичних операцій

На рисунку 1 цифрами позначено наступні етапи:

1. опис електричної схеми ЦС;
2. аналіз ступеню контрольованості ЦС, видача переліку елементів, які не піддаються контролю на друк;
3. доопрацювання схеми ЦС із метою забезпечення її повної контрольованості;
4. синтез тестових наборів;
5. контрольна перевірка, генерування тестових послідовностей;
6. діагностична перевірка, обробка результатів контролю.

Розглянемо сутність запропонованої послідовності (рис.1).

Етап 1. Для введення інформації в ЕОМ, схему об'єкту контролю необхідно описати. Для опису використовуємо наступні позначення:

- множина $A \in (a_1, a_2, a_3, \dots, a_n)$, включає в себе функціональні елементи, які записуються у восьми розрядному коді в довільному порядку;
- множина первинних входів $X \in (x_1, x_2, x_3, \dots, x_x)$ і виходів $Y \in (y_1, y_2, y_3, \dots, y_y)$;
- коди передавальних функцій переходів σ_i входів λ, відповідним елементам $a_j \sigma(\lambda)_i$.

Дуги, які з'єднують елементи A, X, Y між собою, позначаються зазвичай номером того елемента, з якого вони виходять, тому спеціальної множини для їх подання не потрібна.

При опису електричної схеми за номером функціонального елемента вказуються всі дуги, які входять до нього, тобто наводиться сукупність дуг $\overline{U}$ і безліч функціональних елементів A. Елементи опису електричної схеми $A, X, Y, \overline{U}$ характерні для подання орієнтованого графа, тому розглядається як граф.

Функції переходів (виходів) дозволяють аналізувати схему як структурний автомат для визначення фіксованих значень первинних входів, виходів і функціональних елементів, та для побудови тестових послідовностей.

Етап 2. Аналіз контролепридатності ЦС передбачає аналіз графа [8]. При цьому всі параметри A ЦС, умовно розбиваються на підгрупи з вершинами, які відповідають первинним виходам. Прийнявши за достатність контрольованості відповідність під графів деревоподібній структури, необхідно побудувати всі існуючі гілки з корінням в Y_j вершині. Наявність глибоких зворотних зв'язків (ЗЗ) та багато вимірність шляхів (БвШ) свідчить про некоректність схеми в сенсі перевірки. Інформація про некоректні гілки використовується для доопрацювання електричної схеми [9].

Етап 3. Здійснюється доопрацювання електричної схеми ЦС або визначення додаткових контрольних точок безпосередньо в ЦС (якщо це допустимо за умовами виробництва та експлуатації).

Етап 4. Відповідно до обраної схеми контролю ЦС синтез тестів повинен здійснюється з урахуванням можливостей контрольно-діагностичних засобів. Побудова тестів здійснюється для кожного дерева окремо. При цьому одна з гілок вибирається як основний маршрут для перевірки. Ознаки, якими вибирають основний маршрут, можуть бути різними:

- гілка з найбільшою кількістю елементів пам’яті:
- виключно комбінаційна гілка і т.і.

Для обраної гілки будується тестовий набір (послідовність), який забезпечує контроль основного маршруту. Стан первинного входу, елементів гілок та всієї гілки визначається відповідно до функцій переходів (виходів) елементів, які належать контрольованому напряму. Побудований таким чином тестовий набір (або тестова послідовність для гілок з елементами пам'яті) забезпечує перевірку технічного стану лише однієї гілки. Для побудови тестової послідовності для дерева доцільно використовувати діагностичний пристрій (ДП) у вигляді комп’ютерної вимірювальної системи. Генерування тестової послідовності (ТП) полягатиме в визначенні умов порушення перевірки по будь-якій гілці з подальшою переперевіркою основного маршруту за раніше побудованим тестом, який можна назвати початковим.

Етап 5. За результатами перевірки основного маршруту можна зробити висновок про справність пов'язаних із ним гілок. Якщо за порушення умов контрольованості основний маршрут визнано як несправний, то можна зробити висновок про несправності сполучених з ним гілок.

Такий підхід до побудови перевірних ТП та до реалізації контрольних перевірок дає суттєві переваги порівняно з існуючими методами. Різко знижується машинний час синтезу тестових послідовностей, підвищується їх компактність. В результаті знижується вимоги до обсягу оперативної пам'яті ДП, підвищується надійність роботи зовнішніх пристроїв. Прийняття рішення, що до застосування результатів перевірки, можливо в автоматизованому безпосередньо на об'єкті.

Етап 6. Для визначення місця несправності використовується інформація, отримана після здійснення контрольних перевірок. Після перевірки всіх ланцюгів дерева, елементи, які належать гілкам із негативним результатом контролю, вважаються підозрілими. Для того щоб уточнити місце несправності, після перевірки всіх дерев ЦС здійснюється логічна операція перетину $A_i^1 \text{nA}$. В результаті операції перетину кількість підозрюваних елементів буде знижено до групи елементів або одного елемента.

Використання сучасного індукційного методу діагностування, алгоритмів виділення та обробки діагностичної інформації, прийняття рішення про технічний стан (ТС) ОК і місця локалізації несправного компоненту дає змогу розробити функціональну схему автономної системи технічного діагностування (рис. 2).

До її складу входять:

блок живлення (БЖ), що призначений для живлення;

блок виділення діагностичної інформації та її перетворення;

блок управління (БУ);

блок інтерфейсу, для під’єднання ОК та вибору необхідного входу;

блок інтерфейсу для обміну інформацією між датчиками діагностичної інформації, блоком виділення діагностичної інформації, комутатором та сигнальним процесором;

блок індикації (БІ), для реєстрації та індикації результатів «контролю ТС» і «локалізації» несправного радіоелектронного компонента.

Обсяг оперативної пам'яті має забезпечити розміщення не менше одного перевірного тестового набору. До складу системи діагностування (ДП) повинен входити лічильники тестових наборів, що подаються на ЦС.

Для формування (подачі) перевірних послідовностей, а також збереження еталонних реакцій ОК на певну перевірну послідовність, система діагностування повинна містити змінний запам’ятовуючий пристрій. Іншим варіантом є використання штучного інтелекту для створення (генерування) тестових повідомлень, з можливість комутації на відповідні входи об’єкту контролю. Алгоритми роботи ДП доцільно також закладати в змінному пристрої пам’яті, що дає можливість адаптування системи контролю під різноманіття цифрових об’єктів контролю.

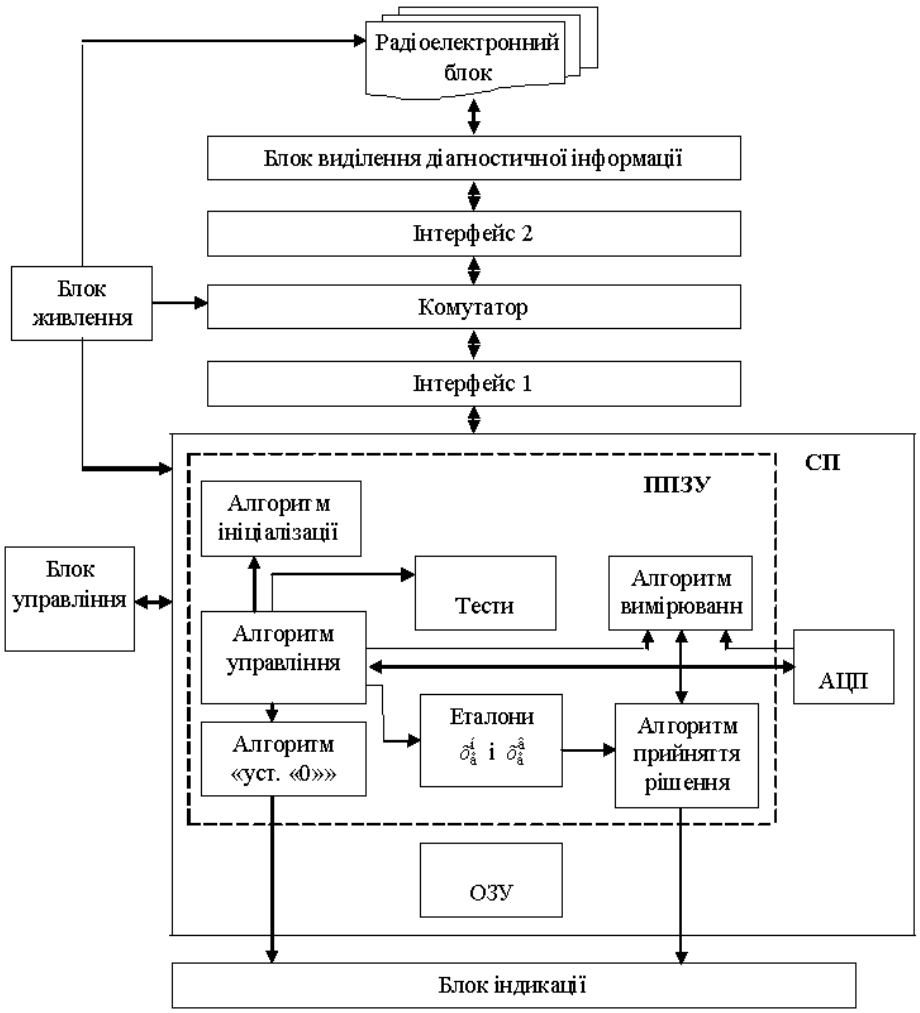


Рис. 2. Структура системи контролю

Висновки. Запропонований метод проведення технічного контролю дозволяє сформувати структурну схему системи автоматизованого контролю технічного стану цифрових систем з використанням спеціально сформованих перевірних тестових послідовностей.

Поєднання математичних алгоритмів з синтезу тестів засобами обчислювальної техніки з можливостями засобів діагностування у вигляді обчислювально-вимірювального комплексу, спрощує процеси контролю та діагностування цифрових систем та покращує ефективність системи контролю.

Список літератури

1. Хорошко В., Кузавков В., Янковський О., Болотюк Ю. Вимоги до засобів діагностування обчислювальних систем. *Безпека інформації*. Київ. 2022. №3 (28). С. 127-132.
2. Шкуліпа П.А. Основні напрямки розвитку автоматизованих систем технічного діагностування об'єктів радіоелектроніки. *Вісник Хмельницького національного університету*. *Технічні науки*. 2012. № 6. С.192-194.
3. Шкуліпа П.А. Методика проведення діагностування аналогових пристроїв динамічним методом. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* К. 2012. № 38. С.106-110.
4. Вишнівський В., Жердєв М., Креденцер Б., Кузавков В., Редзюк Є. Безконтактний індукційний метод діагностування радіоелектронних блоків. *Збірник наукових праць ВІКНУ ім. Тараса Шевченка*. 2013. Вип.43. С.17-23.
5. Чжен Г. Мэннинг Г., Метц Г. Диагностика отказов цифрових вычислительных систем. М.: Мир, 2002. 232с.
6. Гайдур Г., Кузавков В., Редзюк Є., Сєрих С. Безконтактний індукційний метод визначення технічного стану цифрового блока: розрахунок потужності випромінювання провідника. *Зв'язок*. 2016. №1. С. 32-39
7. Кузавков В., Хорошко В., Янковський О. Технічна діагностика складних технічних об'єктів. *Захист інформації*. 2022. Вип.24. №3. С.115-120.
8. Райгородский А.М. Модели случайных графов. М.: МЦНМО, 2017. 144с.
9. Брейловскій Н.Н., Іванченко Е.В., Хорошко А.В. Діагностика системи захисту інформаційного простору. *Захист інформації*. *Спеціальний випуск*. 2014. С. 59-67.

OPTION OF THE SYSTEM FOR DETERMINING THE TECHNICAL CONDITION OF DIGITAL OBJECTS

V.O. Khoroshko, V.V. Kuzavkov, Y.V. Bolotiuk

Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty; 45/1, Kniaziv Ostrozkyh St, Kyiv, 01011, Ukraine
e-mails: professor_va@ukr.net; nevse@ukr.net; yuliia.bolotiuk@viti.edu.ua

The widespread involvement of digital devices (systems) in human activity raises the urgent question of ensuring the reliability of the functioning of such systems. In turn, ensuring reliability is not possible without an effective control system and diagnostics of the technical condition of the selected object of control. On the other hand, the manufacturer of digital equipment is not interested in many years of trouble-free operation of the samples manufactured by him, because this slows down the production cycle and, accordingly, reduces profits. The task of monitoring the technical condition of any digital device rests entirely with the user of the specified means. It is known that in the confrontation between separate control means and unified control systems of digital equipment, unified control systems based on non-contact methods of recording diagnostic information win. The structure of such systems is also known, it is a computer measuring system with specialized software for collecting and processing diagnostic information, as well as an intelligent decision support system. The solutions proposed by the authors are based on a non-contact induction method of diagnosis and a unified diagnostic parameter that reflects the physical and chemical aging processes of semiconductor structures of digital radio electronic components. The application of mathematical methods for building a system of technical diagnostics of digital objects is considered. A generalized method of digital equipment control by constructing verifiable test sequences is presented. The methodology is based on modern methods of obtaining and processing diagnostic information, algorithms for constructing diagnostic tests. The obtained results make it possible to automate the process of determining the actual technical condition of modern digital equipment.
Keywords: diagnostic parameter, model, test, algorithm.

DOI 10.15276/imms.v13.no3-4.349
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 349-359

РОЗРОБКА ЗАХИЩЕНОЇ СИСТЕМИ ДЛЯ ОБМІНУ ДОКУМЕНТАМИ У НАВЧАЛЬНОМУ ПРОЦЕСІ

І.М. Чураков, Н.І. Кушніренко, В.В. Зоріло

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
e-mail: infsec2011@gmail.com

Головним акцентом дослідження є потреба в сучасній та ефективній системі обміну документами між викладачами та студентами. Зміни в освітньому оточенні, структурі та форматі навчального процесу в результаті поширення технологій і зокрема умов пандемії COVID-19 вимагають новітніх рішень. Ефективність навчального процесу та його керованість значною мірою залежать від швидкості, надійності та зручності обміну інформацією між учасниками освітнього процесу. В освітніх закладах щодня циркулюють величезні обсяги інформації від пересилки лабораторних робіт до контрольно-підсумкових завдань. Без сучасних цифрових технологій, цей процес може бути не тільки повільним, але і супроводжуватись втратами, помилками і затримками, тому необхідність системи обміну документами є актуальною на сьогодні. Крім того, великою проблемою для впровадження таких систем є питання інформаційної безпеки, адже обмін документами включає обробку та передачу конфіденційної інформації, яка повинна бути захищена від несанкціонованого доступу та зловмисного використання. У зв'язку з цими викликами, було зосереджено зусилля на розробці системи обміну документами, яка використовує сучасні алгоритми шифрування для безпечної передачі даних. Це дослідження та розробка набули не тільки академічної, а й практичної значимості, оскільки вони заповнюють прогалину між вимогами до сучасного електронного навчання і реальними можливостями освітніх установ в обміні та захисті інформації. Результатом проведеного дослідження стала розробка системи, яка використовує сучасні цифрові технології, такі як двофакторна авторизація, протокол шифрування AES та алгоритм хешування PBKDF2. Розроблена система обміну документами – це практичний внесок в галузь освітніх технологій, який відкриває нові горизонти для автоматизації, ефективності та безпеки в сфері обміну документами в освіті.

Ключові слова: двофакторна авторизація, API-ключі, PBKDF2, безпека даних, управління базою даних, обмін документами, електронне навчання.

Вступ. Ми живемо в епоху електронних технологій та глобалізації, коли цифрові інструменти стають нероздільною частиною як професійної діяльності, так і повсякденного життя [1]. Сучасне освітнє середовище теж не залишається за межами цього тренду. Навчальні заклади в усьому світі активно інтегрують технології в навчальний процес, намагаючись зробити його більш ефективним і доступним.

Одним з найважливіших напрямків цифрового впровадження в освіті є розробка систем обміну документами [2]. Це є необхідною складовою успішного навчального процесу, адже передача документації між студентами, викладачами та адміністрацією стає швидкою та ефективною. Але з ростом кількості персональних та конфіденційних даних, які пересилаються через цифрові канали, виникає проблема забезпечення інформаційної безпеки.

Не можна ігнорувати ризики, пов'язані з потенційними кібератаками чи несанкціонованим доступом до інформації. Тому важливо розуміти, що цифрова

трансформація освіти вимагає не тільки впровадження новітніх технологій, але і розробки ефективних механізмів їх захисту.

Обмін документами в освітній сфері став основою багатьох досліджень. Наприклад, багато таких інструментів як Google Classroom, Moodle та Remind вже успішно використовуються в навчальних закладах. Google Classroom, один з найпопулярніших інструментів, дозволяє викладачам й учням надсилати та отримувати завдання, проводити тести та швидко обмінюватися повідомленнями [3]. Moodle, відкрита система керування курсами, пропонує більш налаштовувану систему з великою кількістю модулів та плагінів, включаючи безпосередній обмін файлами [4]. Remind, сервіс для надсилання повідомлень, дозволяє викладачам й учням миттєво обмінюватися інформацією без розкриття особистих контактних даних [5]. Однак, хоча ці системи вже розширюють можливості обміну документами в освіті, вони можуть бути перевантажені зайвим функціоналом і часто є платними. В той же час більш прості програми не вирішують в повній мірі питання інформаційної безпеки. В даній роботі запропонована система обміну документами, яка забезпечує захист інформації, що в ній циркулює.

Мета статті та постановка завдань. В сучасному світі інформаційних технологій і цифрової глобалізації, область освіти стикається з новими викликами, зокрема, із необхідністю безпечного обміну документами в процесі навчання. Це потребує ретельного вивчення та аналізу, якому ми присвячуємо нашу роботу.

Метою роботи є аналіз та вибір найбільш ефективних засобів для забезпечення безпеки даних в процесі обміну документами, а також розробка та впровадження обраних засобів в систему обміну документами.

Для досягнення поставленої мети необхідно розв’язати наступні *задачі*:

1) Проаналізувати засоби для забезпечення безпеки даних.
2) Оцінити можливості різних систем керування реляційними базами даних.
3) Вибрати спосіб реалізації системи авторизації.
4) Впровадити обрані підходи в розроблювану систему для обміну документами.

Особливий акцент в нашій роботі буде зроблено на питання захисту персональних даних учасників освітнього процесу, оскільки це критично для дотримання принципів конфіденційності та захисту прав людини.

Основна частина. Забезпечення безпеки даних – це один з ключових елементів розробки програмного забезпечення. Це включає в себе шифрування даних, забезпечення цілісності даних, та системи аутентифікації та авторизації.

Серед доступних варіантів наступні вирізняються своїми перевагами та недоліками:

1. Шифрування даних:
    1.1. AES (Advanced Encryption Standard): Стандарт шифрування, використовується урядами, банками та іншими організаціями, яким потрібна висока ступінь захисту даних. Проте, він є складним у використанні і потребує певних навичок для безпечного застосування.
    1.2. RSA (Rivest - Shamir - Adleman): Це широко використовується варіант асиметричного шифрування, що дозволяє безпечне обмін даними. Його недоліком є те, що він повільніший за AES.
2. Хешування даних:
    2.1. PBKDF2 (Password-Based Key Derivation Function 2) дозволяє створити криптографічно безпечний хеш від вхідного пароля. Недоліком є те, що його можна «зламати» з достатньо потужним обчислювальним обладнанням[6].
    2.2. bcrypt: Це ще одна популярна функція хешування для захисту паролів. Вона вважається безпечнішою, але є повільнішою за PBKDF2.

3. Аутентифікація:

3.1. Двофакторна аутентифікація: Це потужний спосіб забезпечити безпеку облікового запису, вимагаючи додаткового кроку підтвердження після введення пароля. Але він також може збільшити складність використання системи для кінцевого користувача.

3.2. Безпечний обмін ключами (наприклад протокол Діффі-Хеллмана). Це дозволяє двом сторонам безпечно обмінюватися ключами по надійному каналу. Недолік – це складність реалізації.

Вибір конкретних методів завжди надає багато простору для обговорення, але для цього проекту вирішено було скористатись шифруванням даних AES, хешуванням PBKDF2 та двофакторною автентифікацією.

AES вважається одним з найбільш надійних алгоритмів шифрування, використовуючи блочне шифрування з ключем довжиною від 128 до 256 біт для надійного захисту даних [7]. Незважаючи на те, що це може бути складніше для реалізації, використання AES забезпечує високий рівень захисту даних.

PBKDF2, у свою чергу, є стандартом для хешування паролів і використовується дуже широко. Його основна перевага полягає в використанні солі для захисту від швидких атак на хеші паролів. Це означає, що навіть якщо зловмисник отримає хеші паролів, йому все одно доведеться витратити значний час і ресурси для злому кожного окремого пароля.

Двофакторна автентифікація, хоча і може здатися складною для користувачів, забезпечує додатковий шар захисту, зменшуючи шанс несанкціонованого доступу до системи навіть у випадку витоку або викрадення пароля.

Таким чином, комбінація обраних нами трьох методів створює ідеальний баланс між надійністю та зручністю користування саме для задач даного проекту.

У контексті обраної нами теми, доцільно розглянути інструмент, який буде гарантувати безпеку даних – систему керування реляційними базами даних (RDBMS).

Система керування реляційними базами даних (RDBMS) – це програмне забезпечення, що дозволяє створювати, оновлювати та керувати реляційною базою даних. На сьогоднішній день є велика кількість RDBMS, серед найпопулярніших: MySQL, PostgreSQL, SQLite, Microsoft SQL Server.

Важливо обрати RDBMS, яка найбільше підходить для проекту, враховуючи такі чинники, як розмір проекту, очікуване навантаження на базу даних, вимоги до професійних навичок розробників, вартість, та багато інших [8]. В табл. 1 приведено порівняльну таблицю деяких з найбільш популярних реляційних СКБД [9], що використовуються сьогодні, з окресленням їхніх основних переваг та недоліків.

Таблиця 1

Порівняльна характеристика систем керування реляційними базами даних

RDBMS	Переваги	Недоліки
MySQL	Універсальність, швидкість, висока продуктивність і стійкість.	Є певні обмеження у функціональності.
PostgreSQL	Гнучкість, велика кількість можливостей, відкритий код.	Складніший в налаштуванні, вимагає більше ресурсів машини.

продовження таблиці 1

SQLite	Невеликий розмір, проста в використанні, не вимагає окремого сервера.	Обмежена місткість, не підходить для великих проектів.
Microsoft SQL Server	Тісна інтеграція з .NET, відмінна підтримка, надійність.	Платна, може бути занадто громіздкою для малих проектів.

Після детального вивчення наведених систем керування реляційними базами даних було вирішено скористатись MySQL для цього проекту.

MySQL є універсальним рішенням, відомим своєю швидкістю, надійністю та стійкістю. Її використовують десятки тисяч веб-сайтів по всьому світу, включаючи таких великих гравців як Facebook, Twitter і YouTube.

Незважаючи на певні обмеження у функціональності, що можуть бути знайдені в інших RDBMS, MySQL надає усі необхідні можливості для ефективного керування даними в рамках цього проекту. Вона має зрозумілий інтерфейс і легко інтегрується з іншими технологіями, що використовуються на проекті.

Вибір MySQL і для цього проекту також обумовлений розглядом таких чинників як розмір та складність проекту, плановане навантаження на базу даних. Однак, організація безпечного зберігання даних - це лише один аспект багатогранного процесу створення надійного і складного проекту. Окрім цього, ефективність системи в значній мірі залежить від правильно вибраної системи авторизації.

Система авторизації є ключовою складовою безпеки будь-якої сучасної системи або додатку. Вона перш за все повинна забезпечити впевненість, що тільки відповідні користувачі мають доступ до відповідних ресурсів. Різні системи мають різні вимоги до авторизації, тому важливо обрати правильний метод, що найкраще відповідає потребам.

Існують такі основні методи реалізації системи авторизації:

• JWT (JSON Web Tokens): цей метод передбачає використання токенів для авторизації користувачів. Безпека JWT провіряється за допомогою підпису токена. Головною перевагою є те, що сервер не потребує зберігати сесію користувача, тобто це без станова авторизація [10].

• Сесії: цей метод передбачає створення унікального ідентифікатора сесії, який зберігається на сервері і використовується для перевірки привілеїв користувача. Цей підхід вимагає більше ресурсів, але надає більший контроль над даними сесії.

• OAuth: це стандарт, що дозволяє користувачам надавати застосункам обмежений доступ до своїх ресурсів на інших сайтах. Це складніший, але більш гнучкий метод авторизації, який широко використовується для розподілених систем [11].

• OTP (One-Time Password): цей метод передбачає використання одноразового пароля, який генерується алгоритмом і має короткий термін дії. OTP надійний, оскільки динамічні паролі важче викрасти, а також не можна використовувати повторно.

Реалізація системи авторизації на основі одноразових паролів (OTP) для цього проекту була обрана з кількох причин.

По-перше, OTP надає високий рівень безпеки в порівнянні зі сталими паролями. Кожний пароль використовується тільки один раз, тому навіть якщо зловмисник перехопить пароль, він не зможе повторно використати його. Це важливо в контексті глобального зростання кіберзлочинності.

По-друге, використання OTP доповнює інші заходи безпеки, що були вибрані для цього проекту. Комбінація OTP і двофакторної аутентифікації створює сильний захист від несанкціонованого доступу.

По-третє, більшість людей вже знайомі з концептом OTP через їх використання в банківському секторі і інших сферах, де вимагається висока безпека. Отже, використання OTP не створить бар'єрів для використання системи кінцевими користувачами.

Ось чому, вимірюючи переваги і недоліки різних систем авторизації, ми вирішили, що OTP наразі найкраще підходить для цього проекту. Але не можна забувати, що ефективна система авторизації повинна також передбачати додаткові рівні захисту, як, наприклад, двофакторна авторизація.

Специфіка 2FA полягає в тому, що для успішної авторизації потрібно надати не тільки щось, що вам відомо (наприклад, пароль), але і щось, що ви маєте (наприклад, мобільний телефон). Це значно підвищує безпеку системи, тому що потенційний зловмисник має не тільки вичислити пароль, але і фізично отримати пристрій користувача [12].

Для цього проекту було обрано комбінований підхід до 2FA, який використовує одноразові паролі (OTP) та програму Google Authenticator.

Принцип роботи Google Authenticator та одноразового пароля [13]:

1. Генерація Ключа. Коли користувач реєструє обліковий запис на підтримуваному веб-сервісі, генерується унікальний секретний ключ. Цей ключ зберігається на сервері веб-служби, а також передається на пристрій користувача, часто у вигляді QR-коду.

2. Сканування QR-коду. Для початкового налаштування Google Authenticator, користувачу необхідно сканувати QR-код своєю мобільною камерою. Цей QR-код містить таємний ключ.

3. Генерування OTP. За допомогою секретного ключа, Google Authenticator генерує шестизначний код OTP. Цей код змінюється кожні 30 секунд. Google Authenticator використовує стандартний алгоритм HMAC-SHA1 для генерації OTP.

4. Введення OTP. Коли користувач намагається увійти в свій обліковий запис, він вводить OTP, показаний в Google Authenticator, разом із своєю поштою та паролем.

5. Перевірка OTP: Після того, як користувач вводить OTP, сервер, з якого було отримано ключ, використовує той же алгоритм, що і Google Authenticator на базі ключа та поточного часу, щоб перевірити вхідний OTP.

6. Автентифікація При успішному введенні OTP: OTP приймається і користувач авторизується в сервіс.

Тим самим, використання Google Authenticator та одноразових паролів для досягнення двофакторної авторизації в системі забезпечує посилений рівень захисту. За такої схеми, навіть якщо зловмисник вдасться отримати основний пароль користувача, він все одно не зможе здійснити несанкціонований вхід, не маючи доступу до конкретного пристрою, на який надіслано OTP. Але важливо згадати, що для забезпечення загальної безпеки системи, необхідно також акцентувати увагу на безпеці інших елементів, таких як, наприклад, API ключі.

Отримання та використання API-ключів є необхідною складовою більшості веб-систем. Однак, неправильне зберігання чи передача API ключів може призвести до серйозних проблем з безпекою, таких як несанкціонований доступ до системи чи витік даних. Тому забезпечення безпеки API ключів є критично важливим.

Одним із способів безпечного зберігання API ключів є їх шифрування перед зберіганням за допомогою надійних шифрувальних алгоритмів. В даному проекті для цього використовується алгоритм AES (Advanced Encryption Standard) [14].

AES – це симетричний алгоритм блочного шифрування, що використовує однакові ключі для шифрування та дешифрування даних. Базова концепція цього алгоритму полягає в заміні, перестановці та перетворенні інформації з метою забезпечення конфіденційності [15].

Для зберігання API ключів використовується такий процес:

- Генерація API ключа. Сервер генерує унікальний API ключ для кожного користувача або сесії.
- Шифрування API ключа. API ключ шифрується за допомогою алгоритму AES за допомогою вибраного ключа шифрування.
- Зберігання шифрованого API-ключа. Шифрований API-ключ зберігається в захищеному місці, такому як база даних або середовище.
- Дешифрування API ключа при використанні. Коли API ключ потрібно використати, він дешифрується за допомогою того ж шифрувального ключа, що й при шифруванні.

За допомогою цього підходу, API ключі зберігаються на сервері в безпечному вигляді і можуть бути безпечно передані через комунікаційні канали, забезпечуючи конфіденційність і цілісність даних.

Хоча AES є потужним алгоритмом шифрування, використовуваним у багатьох сучасних системах, існують інші алгоритми шифрування, які також можуть бути застосовані в залежності від специфічних вимог до безпеки.

В кожному випадку при виборі алгоритму шифрування важливо врахувати ряд параметрів, таких як тип шифрування (симетричний або асиметричний), розмір ключа та розмір блоку. Розмір ключа є важливим аспектом, який визначає рівень безпеки шифрування - більший розмір ключа збільшує кількість можливих ключів і мінімізує ризик злому шляхом «прямого пошуку».

Як приклад, в таблиці 2 наведено ряд алгоритмів шифрування та їх ключові характеристики:

Таблиця 2

Порівняння основних алгоритмів шифрування

Алгоритм	Тип	Розмір ключа	Розмір блоку
AES	Симетричний	128, 192 або 256 біт	128 біт
DES	Симетричний	56 біт	64 біт
Triple DES	Симетричний	112 або 168 біт	64 біт
RSA	Асиметричний	1024 або 2048 біт	Змінний по блокам
ElGamal	Асиметричний	1024 або 2048 біт	Змінний по блокам
Blowfish	Симетричний	32-448 біт	64 біт

Використовуючи зазначені вище технології, було розроблено програму на платформі Windows Forms спеціально для потреб викладачів. Ця програма спрямована на значне поліпшення процесу обміну документами між викладачами та студентами, пропонуючи цілий ряд функціональних можливостей.

Центральними елементами програми є системи реєстрації та аутентифікації користувачів. Алгоритм зашифрованої системи реєстрації обробляє всю необхідну інформацію та зберігає її в базі даних MySQL, використовуючи для цього стандарт AES. Тимчасом, двофакторна система аутентифікації, що ґрунтується на One-Time Password (OTP) та Google Authenticator, забезпечує високий рівень безпеки користувачів' даних.

Програмний продукт, який було розроблено, є сучасною та ефективною системою для управління студентською базою даних та спілкування зі студентами.

У програмі реалізовані логін та реєстрація для забезпечення зручності та безпеки користувачів. При цьому, програма представляє три ключові функціонали.

Додавання студентів в базу даних. В даному розділі програми користувачеві надається можливість вносити інформацію про студентів, а також прив'язувати їх до відповідних груп і предметів. Це забезпечує легкість управління та зручне пошук інформації про кожного студента. Форму з реалізацією даного функціоналу зображено на рисунку 1.

Відправка електронних листів студентам. В цьому розділі програми користувачеві надається можливість автоматично відправляти листи студентам з прикріпленими файлами, а також відправляти завдання у випадковому порядку. Це полегшує процес взаємодії зі студентами і забезпечує їх оперативне інформування. Форму з реалізацією даного функціоналу зображено на рисунку 2.

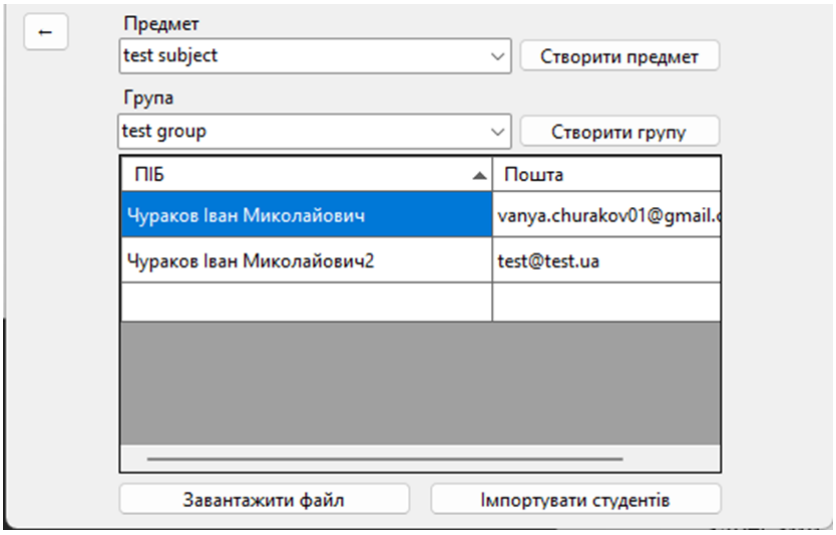


Рис. 1. Форма імпорту студентів

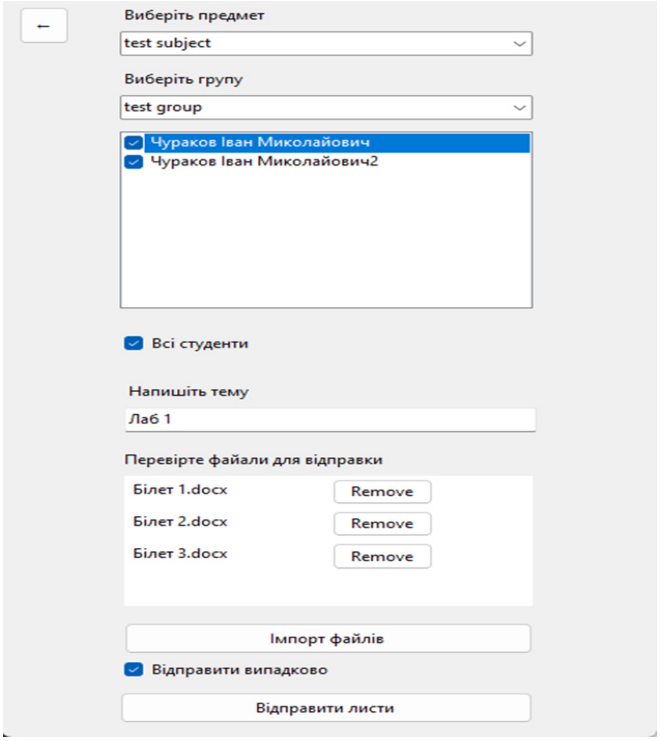


Рис. 2. Форма відправки листів

Перегляд відправлених завдань. У цьому розділі програма надає можливість переглядати, кому були відправлені які завдання та які студенти вже здали свої роботи. Це дозволяє контролювати процес виконання завдань та забезпечує зворотний зв'язок. Форму з реалізацією даного функціоналу зображено на рисунку 3.

Так при обмежених ресурсах, але з врахуванням сучасних технологій ми змогли розробити ефективний та надійний продукт.

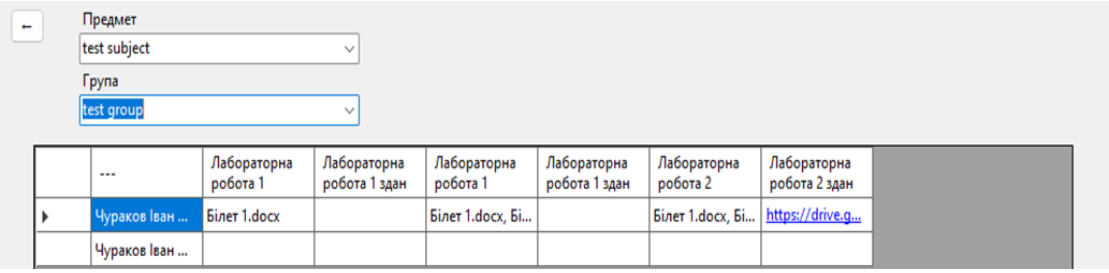


Рис. 3. Форма дошки статусів

Висновки. В роботі проведена розробка системи для захищеного обміну документами між викладачем та студентами.

Для досягнення поставленої мети було розв’язано наступні задачі:

1. Виконано аналіз сучасних рішень для автоматизації документообігу в навчальному процесі. Виявлено, що існуючі програмні рішення зазвичай перенавантажені зайвим функціоналом, а більш прості програми не завжди у повній мірі забезпечують захист конфіденційних даних користувачів.
2. Виконано аналіз сучасних технологій, які застосовуються для розробки захищеного програмного забезпечення. Для розроблюваної системи обрано багатофакторну аутентифікацію за допомогою Google Authenticator для підвищення ступеня захисту системи, що реалізує додатковий рівень перевірки автентифікації користувача. Було проаналізовано та застосовано алгоритм шифрування AES для зберігання API-ключів з метою безпечного зберігання цих ключових ідентифікаторів, що мінімізують ризик непередбаченого витоку конфіденційних даних. Впроваджено алгоритм PBKDF2 для хешування паролів.
3. Розроблена система має наступні можливості:
   - реєстрація користувачів;
   - імпорт та редагування даних студентів та груп;
   - відправка електронних листів студентам;
   - відправка файлів в різних форматах. підтримка відправки в звичайному і випадковому режимах; можливість зберігання документів викладачів в хмарному сховищі;
   - можливість завантаження студентами результатів робіт у вигляді файлів в виділену папку в хмарному сховищі;
   - перегляд відправлень та статусів виконання завдань на дошці статусів.

Як підсумок, можемо зазначити, що запропонована система автоматизує рутинний процес обміну документами між викладачами та студентами і тим самим дозволяє зекономити час та мінімізувати ймовірність помилки, при цьому забезпечується захист конфіденційної інформації користувачів. Розроблений програмний продукт має зручний та інтуїтивно зрозумілий інтерфейс. В якості елементів системи було використано сучасне відкрите програмне забезпечення. Дана система є гнучкою та легко масштабується, що дозволяє шляхом невеликих змін адаптувати її до інших сфер.

Список літератури

1. Vincent J. Life stage or Age. Reviewing perceptions of oldest digital technologies users. *Digital Ageism*. 2023. P. 36-52. DOI:10.4324/9781003323686-3.
2. Bejinaru R. Impact of digitalization on education in the knowledge economy. *Management Dynamics in the Knowledge Economy*. 2019. V.7.3. P. 367-380.
3. About Classroom. URL: https://support.google.com/edu/classroom/answer/6020279?hl=en
4. Features. URL: https://docs.moodle.org/403/en/Features
5. A New Chapter Begins. URL: https://www.remind.com/parentsquare
6. Ertaul L., Manpreet K., Venkata A.K.R. Gudise. Implementation and performance analysis of pbkdf2, bcrypt, scrypt algorithms. *Proceedings of the international conference on wireless networks (ICWN)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2016. http://borg.csueastbay.edu/~lertaul/PBKDFBCRYPTCAM READYICWN16.pdf
7. Singh A. Comparative study of DES, 3DES, AES and RSA. *Int. J. Comput. Technol*. 2013. V.9.3. P. 97-102.
8. Hong S. Big Data: how to choose the right cloud infrastructure. 2016. URL: https://www.researchgate.net/publication/305495731_Big_Data_how_to_choose_the_right_cloud_infrastructure
9. Khawar I. Huge and Real-Time Database Systems: A Comparative Study and Review for SQL Server 2016, Oracle 12c & MySQL 5.7 for Personal Computer. *Journal of Basic & Applied Sciences*. 2017. No.13. P. 481-490.
10. Rajat S. Understanding JSON Web Token Authentication. URL: https://medium.com/p/a1febf0e15
11. Polu S. K. OAuth based Secured authentication mechanism for IoT Applications. *International Journal of Engineering Development and Research (IJEDR)*. 2018. V.6. No.4. P. 409-414.
12. Reese K., Smith T., Dutson J., Armknecht J., Cameron J., Seamons K. A usability study of five {two-factor} authentication methods. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019. URL: https://www.usenix.org/system/files/soups2019-reese.pdf
13. Tilak L. Google Authenticator and how it works? URL: https://medium.com/@tilaklodha/google-authenticator-and-how-it-works-2933a4ece8c2
14. Chappel S. Hiding in Plain Sight: A Guide to Keeping Your API Keys Safe. URL: https://medium.com/@sams-scripts/hiding-in-plain-sight-a-guide-to-keeping-your-api-keys-safe-2fba0373d7a8
15. Rijmen V., Daemen J. Advanced encryption standard. *Proceedings of federal information processing standards publications, national institute of standards and technology* 2001. V.19. s.22. URL: https://jima.me/wp-content/uploads/2016/05/Advanced-Encryption-Standard-Wikipedia-the-free-encyclopedia.pdf

І.М. Чураков, Н.І. Кушніренко, В.В. Зоріло

DEVELOPMENT OF A SECURE SYSTEM FOR DOCUMENT EXCHANGE IN THE EDUCATIONAL PROCESS

I. Churakov, N. Kushnirenko, V. Zorilo

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
e-mail: infsec2011@gmail.com

The main focus of the study is the need for a modern and efficient system of document exchange between teachers and students. Changes in the educational environment, structure and format of the educational process as a result of the spread of technology and, in particular, the COVID-19 pandemic require the latest solutions. The effectiveness of the educational process and its manageability largely depend on the speed, reliability and convenience of information exchange between participants in the educational process. Educational institutions exchange huge amounts of information on a daily basis, from moving homework to final exams. Without modern digital technologies, this process can be not only slow, but also accompanied by losses, errors and delays, so the need for a document exchange system is relevant today. In addition, information security is a major anchor for the implementation of such systems, as document exchange involves the processing and transmission of sensitive information that must be protected from unauthorized access and misuse. In response to these challenges, efforts have been focused on developing a document exchange system that uses modern encryption algorithms for secure data transmission. This research and development has acquired not only academic but also practical significance, as it fills the gap between the requirements for modern e-learning and the real capabilities of educational institutions in the exchange and protection of information. The result of the conducted research was the development of a system that uses modern digital technologies, such as two-factor authentication, the AES encryption protocol, and the PBKDF2 hashing algorithm. The developed document exchange system is a practical contribution to the field of educational technologies, which opens new horizons for automation, efficiency and security in the field of document exchange in education.

Keywords: two-factor authentication, API keys, PBKDF2, data security, database management, document exchange, e-learning.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 13, номер 3-4, 2023. Одеса – 360 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 13, номер 3-4, 2023. Одесса – 360 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 13, No. 3-4, 2023. Odesa – 360 p.

Засновник: Національний університет «Одеська політехніка»

Зареєстровано Міністерством юстиції України 04.04.2011р.
Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Національного університету «Одеська політехніка», (протокол № 7 від 19.12.2023р.)

Адреса редакції: Національний університет «Одеська політехніка»,
проспект Шевченка, 1, Одеса 65044 Україна

Web: www.immm.op.edu.ua (immm.opu.ua)

E-mail: immm.ukraine@gmail.com