УДК 004.8:378 DOI: 10.31673/2786-8362.2025.012293

Легомінова С.В., д.е.н.; **Щавінський Ю.В.,** к.т.н.;
Бударецький Ю.І., к.т.н.; **Будзиньский О.В.**

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR AUTOMATED ASSESSMENT OF SITUATIONAL TASKS IN CYBERSECURITY TRAINING

Lehominova S.V., Shchavinsky Yu.V., Budaretsky Yu.I., Budzynskyi O.V. Application of artificial intelligence for automated assessment of situational tasks in cybersecurity training. The article considers the problem of objective assessment of students' success in performing situational tasks in higher education institutions, in particular in conditions of distance and blended learning. Analysis of scientific publications indicates the influence of the contrast effect during assessment and the risks of subjectivity inherent in traditional assessment methods. An automated assessment tool is proposed, based on semantic comparison of students' answers with a reference answer, using natural language processing (NLP) technologies and a mathematically based sentence transformer model. Based on standard Python libraries, an improved model for automatic assessment of text situational tasks has been developed, which performs a comprehensive analysis of the semantic and lexical coherence and completeness of students' answers in comparison with the reference answer. Modeling and testing demonstrated a high Pearson correlation coefficient (>0.95) between the scores generated by the model and expert assessments, which confirms the accuracy and reliability of the results. A key advantage of the model is its ability to detect internal plagiarism in student responses, thus supporting academic integrity. The model also significantly reduces the time required for grading compared to traditional approaches and allows for visualization of potential similarities.

Keywords: information technology, artificial intelligence, situational learning, automatic assessment, cybersecurity

Легомінова С.В., Щавінський Ю.В., Бударецький Ю.І., Будзинський О.В. Застосування штучного інтелекту для автоматизованого оцінювання ситуативних завдань у навчанні кібербезпеки. У статті розглядається проблема об'єктивного оцінювання результатів виконання ситуативних завдань кібербезпеки. Аналіз наукових публікацій виявив труднощі оцінювання великого обсягу текстових відповідей, впливом ефекту контрастності при оцінюванні і ризиками суб'єктивізму під час традиційного оцінювання. Запропонований метод застосування штучного інтелекту для оцінювання, побудована розширена модель оцінювання з використанням стандартних бібліотек мови програмування Python. Перевагою моделі є визначення внутрішнього плагіату між відповідями студентів з метою дотримання академічної доброчесності, значне скорочення часу оцінювання у порівнянні з традиційним підходом та візуалізація можливих збігів.

Ключові слова: інформаційні технології; штучний інтелект; ситуативне навчання; автоматичне оцінювання; кібербезпека

Introduction

Statement of the problem. In the modern higher education environment, information technologies (IT) play a crucial role in transforming traditional learning methods. Situational learning in the training of cybersecurity specialists offers numerous advantages, yet it also faces a number of challenges. The continuous evolution of technology and the emergence of new threats require the regular updating of scenarios. It is essential to provide detailed and constructive feedback to students after task completion. The use of real or simulated data may raise ethical concerns, especially when sensitive or confidential information is involved. Therefore, as most researchers emphasize, teachers must have a high level of competence and be proficient in modern means and methods of information technology for teaching [1] . The need to assess extensive textual data particularly when dealing with a large number of students places a significant burden on instructors and increases the risk of subjective grading. Unlike standardized tests, situational responses do not have a single correct answer, complicating the development of clear and fair evaluation criteria. Additionally, there remains the risk of the contrast effect, where an instructor may unintentionally assess a student's response in relative rather than absolute terms, for instance, after reading a particularly strong or weak previous answer [2]. In the distance-learning format, it is much more difficult to detect plagiarism or suspiciously similar student responses to situational tasks that are not automatically checked by

traditional testing tools [3]. Under these conditions, there is a growing need for new approaches to assessing situational tasks, in particular through the use of artificial intelligence (AI), natural language processing (NLP), content-based automatic grading systems and visualizations of response similarity to detect potential plagiarism.

Analysis of recent studies. Taking into account the challenges related to manual coding and identifying student achievements, as well as the limitations of existing methods for automatic identification and assessment of student performance, study [4] developed an effective tool for identifying and evaluating cognitive presence in online discussion forums. The study applied a methodology that integrates Random Forest (RF) classification with TF-IDF feature extraction and Support Vector Machine (SVM) classification with embedded Word2Vec. According to the researchers, this ensemble method demonstrated notable efficiency, although it achieved only 69% accuracy in classification tasks.

In study [5], the challenges of applying situational learning for students majoring in Cybersecurity were identified. These include the difficulty of creating realistic scenarios, the need for substantial time and resource investments, the requirement to develop specialized programs and ensure high instructor qualifications, the complexity of defining clear criteria for evaluating situational task responses, and the necessity to use AI to advance and refine the situational learning method.

In study [6], a model of situational cognitive learning in the context of network information security was developed. Based on the results of simulation modeling, the authors concluded that the situational learning method can maximize the benefits of balanced control over learning resources, reduce economic losses, and optimize the situational cognitive learning model itself. The importance of prompt response to situations and effective decision-making in the field of cybersecurity highlights the need to apply and further develop this method in higher education institutions during the training of information and cybersecurity professionals. In study [7], the authors analyzed existing approaches to situational awareness in cybersecurity and found that these approaches typically offer semi-automated or entirely manual solutions, which significantly depend on human interaction and thus affect the speed and efficiency of threat response. Another critical issue is the time-consuming and subjective nature of evaluating a large volume of student responses to situational tasks, especially in distance learning settings. The attempts initiated in study [8] to automate the evaluation of large volumes of text using a modeling method that considers contextual cues to derive correct meanings for polysemous words revealed the challenge of accurately assessing multi-word expressions.

A comprehensive review conducted in study [9] on automatic short answer grading (ASAG) systems demonstrated significant advancements in assessment methods for short answers, while also identifying the persistent problem of scaling up to evaluate large volumes of assignments and the necessity for continued research into effective solutions for this challenge.

The analysis of the scientific literature and the identified problems in applying the situational learning method show that the rapid expansion of distance and blended learning formats, supported by information technologies, necessitates the search for ways to automate the prompt evaluation of numerous possible solutions to situational tasks.

The purpose of this paper is to develop, test, and implement an automated approach using AI for assessing situational tasks in higher education, which ensures objectivity, scalability, and academic integrity in the context of distance and blended learning.

To achieve the goal, the following tasks have been identified:

- to analyze existing approaches to the automated assessment of open-ended responses and situational tasks using AI;
- to develop requirements for an answer evaluation system, taking into account criteria of objectivity, scalability, and the assurance of academic integrity;
- to create or adapt AI models for processing, semantic analysis, and assessment of student responses;
- to implement a plagiarism detection module for comparing student responses with model (reference) answers;

- to pilot the proposed approach on a sample group of students, analyze the results, and compare them with traditional expert evaluation.

Presentation of the main research material

Theoretical basis of the application of artificial intelligence in the assessment of situational tasks. One of the promising approaches to solving this problem is the use of AI technologies, in particular NLP, machine learning and neural network models. According to the researchers' conclusions, automatic assessment of open-ended responses allows achieving an acceptable level of accuracy and correlation with expert assessments, provided that the model is properly configured and the criteria are selected [6, 10]. AI technologies enable the implementation of a semantic approach to assessment. Unlike simple sample or keyword matching, such systems analyze the semantic similarity between student responses and reference answers. One of the most effective technologies for this purpose is Sentence-BERT models, which generate vector representations of sentences and allow for the computation of their similarity using the cosine similarity metric [11]. Cosine similarity is a metric that measures the angular similarity between two vectors in a multidimensional space using the following formula

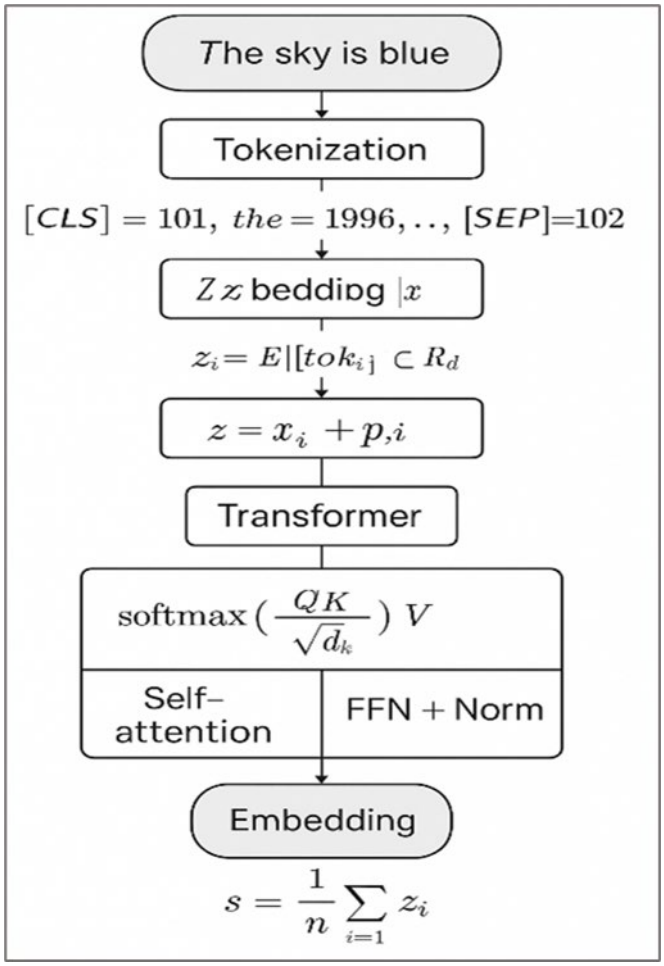


Fig. 1. Algorithm SentenceTransformer

$$cosine_{similarity(A,B)} = \frac{A * B}{\|A\| * \|B\|} \quad (1)$$

where: A and B are text vectors (embeddings); $A * B$ is the scalar product of vectors; $\|A\| * \|B\|$ are the norms (lengths) of vectors.

The transformation of text into embeddings is a mathematical process based on neural networks, particularly on transformer architectures, such as BERT, RoBERTa, and Sentence-BERT. A

simplified algorithm of such a transformation, using the sentence "The sky is blue" as an example, is illustrated in Figure 1. The model splits each sentence into parts (tokens). Each token receives a numerical representation that takes context into account where [*CLS*] and [*SEP*] are the service tokens of the beginning and end, «The, sky, is, blue» – have their numerical indices. Each token is converted into a vector of dimension space R^d. To make the model know the order of words (positions), a position vector is added to each vector $z = x_i + p_i$, where x_i is the token vector, p_i is the position vector i.

In the classic transformer block, the following are calculated

$$Attention(Q,K,V) = soft\max\left(\frac{Q*K}{\sqrt{d_k}}\right)*V\,, \tag{2}$$

where: *Q, K, V* - are matrices of queries, keys and values obtained from x_i; *dk* is the dimension of the keys; *softmax* provides weights for the combination of input vectors.

After calculating *Attention*, each vector is processed through a conventional neural network using the Feed-Forward Neural Network (FFN) formula, which is used inside each transformer layer

$$FFN(h) = \mathrm{Re}\,LU(h*W_1 + b_1)*W_2 + b_2 \tag{3}$$

The values of the Feed-Forward Neural Network components and the calculation steps are shown in Table 1.

Table 1

Contents and calculation steps Feed-Forward Neural Network

Part	Meaning	Explanation
h	Input vector	For example, this is the result of self-attention
W_1, b_1	First layer parameters	Weight matrix and offset vector for the first transformation.
$h \cdot W_1 + b_1$	Linear transform	Multiply the input by the weights and add the offset.
ReLU(...)	ReLU activation	Replace all negative values with zero and add nonlinearity.
W_2, b_2	Second layer parameters	New weight matrix and offset after ReLU.
$ReLU(...)*W_2 + b_2$	Second linear transform	Transform after activation and get the FFN output.

The essence of formula (3) is to nonlinearly transform the input feature vector *h*, to strengthen or change its structure before further processing. After all transformations, new vectors z_i are obtained for each token. A single vector for the entire sentence (text) is obtained by averaging (pooling) all vectors

$$s = \frac{1}{n}\sum_{i=1}^{n} z_i\,, \tag{4}$$

where *n* is the number of tokens.

A schematic diagram of the sequence of converting sentences into embeddings is shown in Figure 2.

Embedding is obtained as a result of passing a word or sentence through a transformer

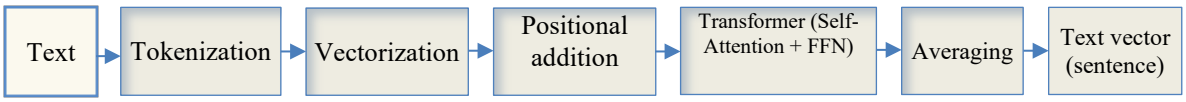


Fig. 2. Sequence diagram for converting a sentence into an embedding

architecture with many layers (Fig. 3).

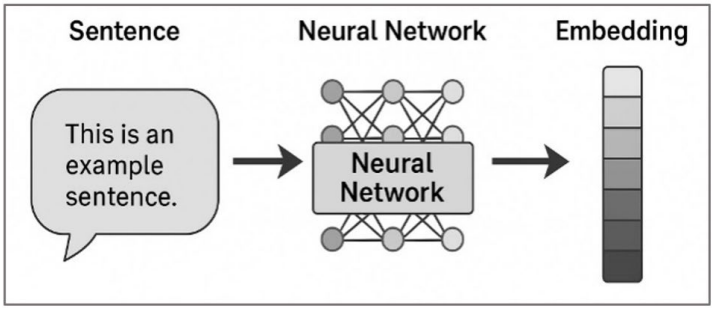


Fig. 3. Sequence diagram for converting a sentence into an embedding

Thus, each student's answer is transformed into a vector (semantic representation), compared with the reference vector (the sample answer), and a similarity score (ranging from 0 to 1) is calculated using formula (1).

Semantic comparison (using SentenceTransformer) allows for detecting similarity in meaning, even when sentence structure or wording differs. This enables the model to assess similarity at the level of meaning. Semantic comparison ensures accurate similarity evaluation, even if the texts differ slightly in wording or structure.

Lexical comparison (e.g., using the Jaccard library in Python or exact text matching) helps detect literal identity of texts (e.g., completely identical sentences). This is important in cases where the answers are indeed the same, but the system might consider them different due to formatting or minor changes. Lexical comparison ensures that fully identical texts do not receive a low score due to formatting or insignificant differences.

A combined scoring approach gives higher scores for semantically similar texts and also accounting for exact matches where necessary.

This approach allows for:

- detecting plagiarism even with minor variations in phrasing;
- identifying exact matches when texts are completely identical.

Such methods are already successfully used in general and professional education contexts. However, their application in highly specialized fields such as cybersecurity requires adaptation – including the creation of domain-specific text corpora, harmonization of terminology, and the development of multi-component reference standards.

Therefore, the integration of AI into the assessment system requires both technological and pedagogical integration.

Creation of a model of automated answer assessment based on artificial intelligence. To achieve this goal, a specialized Python-based software environment was created using the following libraries:

- *SentenceTransformer* to calculate the semantic similarity between the student's answer and the reference answer;
- *pandas* and *openpyxl* to process the results and form a summary table of grades;
- *networkx* and *matplotlib* to build a graph of similarity between students answers in order to detect potential plagiarism;
- libraries for processing text in files of various formats (.txt, .docx, .pdf).

The full listing of the model code is available on GitHub at the link https://github.com/yrii173/StudentAnswerGrading.

The developed assessment model is based on the application of AI methods, particularly deep learning models for natural language analysis, which enable both semantic and lexical comparison of students' textual responses with reference answers, as well as the detection of signs of borrowing (plagiarism) between responses. A key advantage of the model is the ability to export results in Excel format, including the assigned score, the degree of similarity to the reference answer, and a list of suspiciously similar student responses based on pairwise comparison. Visualization of the results is implemented through clustering and marking responses at risk of plagiarism in graphical

representations, where graphs display student responses as nodes and similarity weights as edge labels.

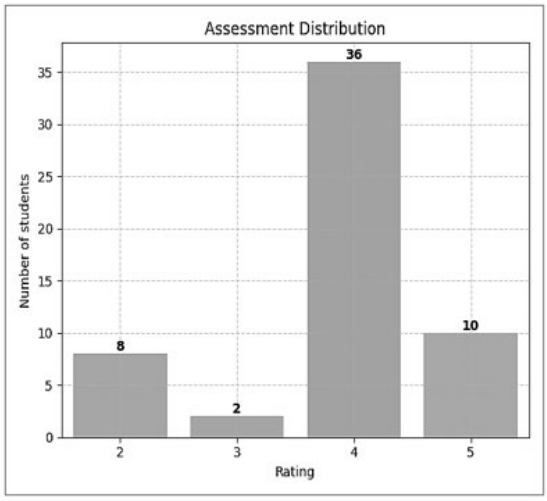
The study of the developed model was conducted in the context of distance and blended learning with students of specialty 125 "Cybersecurity and Information Protection." The evaluation was carried out using previously graded situational tasks with an open structure and detailed textual responses to simulated professional scenarios. To test the model, a folder structure was created containing the model code, student responses, and the reference answer, as illustrated in Figure 4.

```
Ozinka
├── AI_Grading_Example/          #  Student response folder
│       ├── Artemenko.docx
│       ├── Babenko.docx
│       ├── Dariy.docx
│       ……
│       ├── Ivanchenko.pdf
│       ……
│       ├── Zavedeja.docx
├──Zrazok.docx                   #  Reference response file
│
├── PythonApplication1/          #  Project file folder
│       ├── PythonApplication1.py
│       ├── PythonApplication1.pyproj
│       ……
│       ├── results_grading.xlsx  #  Evaluation results output file
```

Fig. 4. Model folder and file structure

All answers were of different sizes from 2 to 4 A4 text pages and were stored as separate text files of different formats in Google Classroom. A previously prepared sample (standard) of the correct answer was used for evaluation.

For the experiment, a database of 56 students' answers to situational tasks was collected. The developed system allowed to process all students' answers within a few minutes, which significantly reduced the time for checking. The evaluation results are shown in Figure 5.



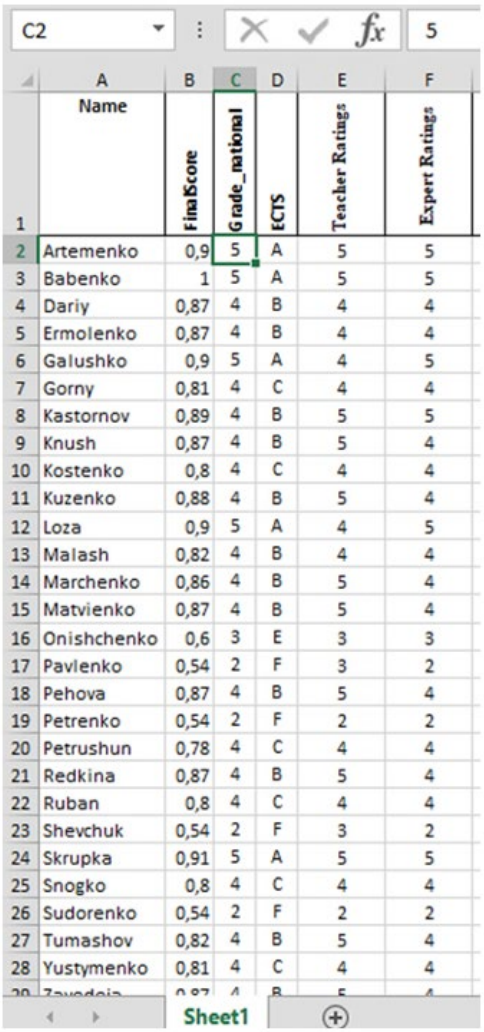
J4

	A	B	C	D	E	F	G	H
1	Name	Similarity	Completeness	LexikaSimilarity	FinalScore	Grade_national	ECTS	PlagiarismWith
2	Artemenko	0,967	0,967	0,268	0,9	5	A	Galushko, Loza
3	Babenko	1	1	1	1	5	A	-
4	Dariy	0,948	0,948	0,213	0,87	4	B	Matvienko, Pehova, Redkina, Zavedeja
5	Ermolenko	0,944	0,944	0,207	0,87	4	B	-
6	Galushko	0,967	0,967	0,269	0,9	5	A	Artemenko, Loza
7	Gorny	0,879	0,879	0,147	0,81	4	C	-
8	Kastornov	0,965	0,965	0,208	0,89	4	B	-
9	Knush	0,945	0,945	0,213	0,87	4	B	Kostenko, Tumashov
10	Kostenko	0,875	0,875	0,167	0,8	4	C	Knush, Tumashov
11	Kuzenko	0,952	0,952	0,184	0,88	4	B	-
12	Loza	0,967	0,967	0,268	0,9	5	A	Artemenko, Galushko
13	Malash	0,899	0,899	0,137	0,82	4	B	-
14	Marchenko	0,939	0,939	0,179	0,86	4	B	-
15	Matvienko	0,948	0,948	0,213	0,87	4	B	Dariy, Pehova, Redkina, Zavedeja
16	Onishchenko	0,655	0,655	0,121	0,6	3	E	-
17	Pavlenko	0,602	0,602	0,008	0,54	2	F	Shevchuk, Sudorenko
18	Pehova	0,948	0,948	0,213	0,87	4	B	Dariy, Matvienko, Redkina, Zavedeja
19	Petrenko	0,6	0,6	0,01	0,54	2	F	-
20	Petrushun	0,856	0,856	0,101	0,78	4	C	-
21	Redkina	0,948	0,948	0,213	0,87	4	B	Dariy, Matvienko, Pehova, Zavedeja
22	Ruban	0,872	0,872	0,178	0,8	4	C	-
23	Shevchuk	0,602	0,602	0,008	0,54	2	F	Pavlenko, Sudorenko
24	Skrupka	0,979	0,979	0,285	0,91	5	A	-
25	Snogko	0,873	0,873	0,129	0,8	4	C	-
26	Sudorenko	0,602	0,602	0,008	0,54	2	F	-
27	Tumashov	0,895	0,895	0,151	0,82	4	B	Knush, Kostenko
28	Yustymenko	0,889	0,889	0,139	0,81	4	C	-

a) *b)*

Fig. 5. Results of evaluating student responses a) score ratio chart, b) output of results to Excel

To confirm the reliability of student answer evaluation performed by the artificial model (based on embeddings and cosine similarity), and to verify the consistency, accuracy, and justification of the scores, an expert group consisting of three cybersecurity professionals was formed. The results of expert evaluation (Expert Ratings) of student responses, along with the instructor's previous evaluations (Teacher Ratings) and the model's evaluation (Grade_national), are presented in Figure 6.



C2 : 5

	A	B	C	D	E	F
1	Name	FinalScore	Grade_national	ECTS	Teacher Ratings	Expert Ratings
2	Artemenko	0,9	5	A	5	5
3	Babenko	1	5	A	5	5
4	Dariy	0,87	4	B	4	4
5	Ermolenko	0,87	4	B	4	4
6	Galushko	0,9	5	A	4	5
7	Gorny	0,81	4	C	4	4
8	Kastornov	0,89	4	B	5	5
9	Knush	0,87	4	B	5	4
10	Kostenko	0,8	4	C	4	4
11	Kuzenko	0,88	4	B	5	4
12	Loza	0,9	5	A	4	5
13	Malash	0,82	4	B	4	4
14	Marchenko	0,86	4	B	5	4
15	Matvienko	0,87	4	B	5	4
16	Onishchenko	0,6	3	E	3	3
17	Pavlenko	0,54	2	F	3	2
18	Pehova	0,87	4	B	5	4
19	Petrenko	0,54	2	F	2	2
20	Petrushun	0,78	4	C	4	4
21	Redkina	0,87	4	B	5	4
22	Ruban	0,8	4	C	4	4
23	Shevchuk	0,54	2	F	3	2
24	Skrupka	0,91	5	A	5	5
25	Snogko	0,8	4	C	4	4
26	Sudorenko	0,54	2	F	2	2
27	Tumashov	0,82	4	B	5	4
28	Yustymenko	0,81	4	C	4	4

Sheet1

Fig. 6. Rating ratio

To validate the experimental results, a statistical correlation analysis tool was used to examine each pair of measurement variables and determine the relationship between the models, teachers, and experts scores. In other words, it was necessary to establish whether the model correctly evaluates the best and highest-quality student responses–specifically, whether high expert scores tend to be associated with high model scores. The result of the statistical analysis was calculated using the Pearson correlation coefficient, according to the following formula:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i = \overline{x}) * (y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i = \overline{x})^2 * \sum_{i=1}^{n}(y_i - \overline{y})^2}}, \quad (5)$$

where x_i, y_i – are the values of paired variables; $\overline{x}$, $\overline{y}$ – are their average values; n – is the sample size summarized in a correlation matrix (Table 2).

Analysis of Table 2 indicates a strong correlation (0.9585306), calculated by formula (5), between expert assessments and model assessments, which confirms the adequacy and validity of the

developed model for assessing students' text responses in distance and blended learning environments. A lower correlation between the teacher's and experts' assessments (0.7831578), as well as between the teacher's and the model's assessments (0.7679357), supports the hypothesis of a contrast effect in the teacher's evaluation – a psychological influence where a very good answer affects the teacher's perception of the next response, which may be of lower quality, or vice versa. Students who submitted answers following particularly strong or weak responses may have received subjectively inflated or deflated scores during manual evaluation.

Table 2

Correlation matrix

	Teacher Ratings	Expert Ratings	Grade_national
Teacher Ratings	1		
Expert Ratings	0,7831578	1	
Grade_national (model)	0,7679357	0,9585306	1

As shown in Figure 6, this effect is especially evident near the boundaries between grade levels. The implementation of automated assessment eliminated this factor, ensuring equal evaluation conditions for all students. In addition to objectivity, a significant advantage of using the model is the substantial time savings in conducting assessments, as illustrated in Figure 7.

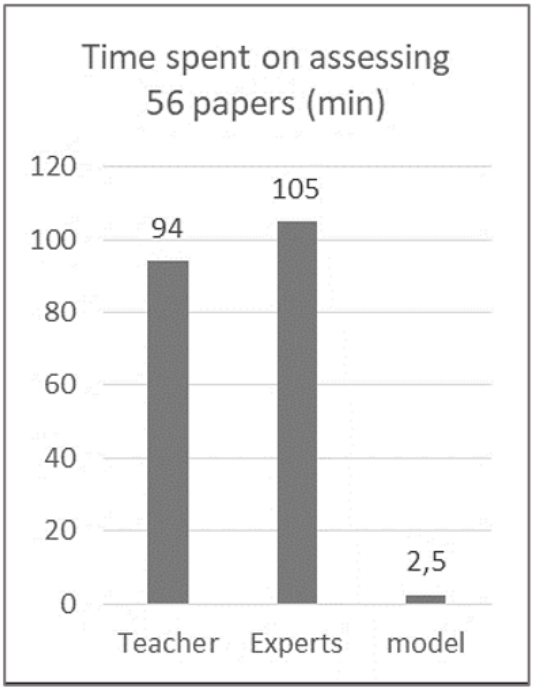


Fig. 7. Evaluation time chart

A distinctive feature of the developed model is the automated comparison of each student response to detect internal plagiarism, which poses a significant challenge for instructors due to the large number of written responses to situational tasks.

Therefore, the model includes a code block for pairwise comparison of responses. For visualization, the model generated a similarity graph of responses (Figure 8), where the nodes represent individual responses and the edges indicate pairs with a high similarity coefficient. The results confirmed the effectiveness of using modern IT tools for automated assessment of open-ended situational tasks in higher education. The developed model demonstrated not only a high level of agreement with expert evaluation but also significantly reduced the time and cognitive load on instructors for reviewing textual responses.

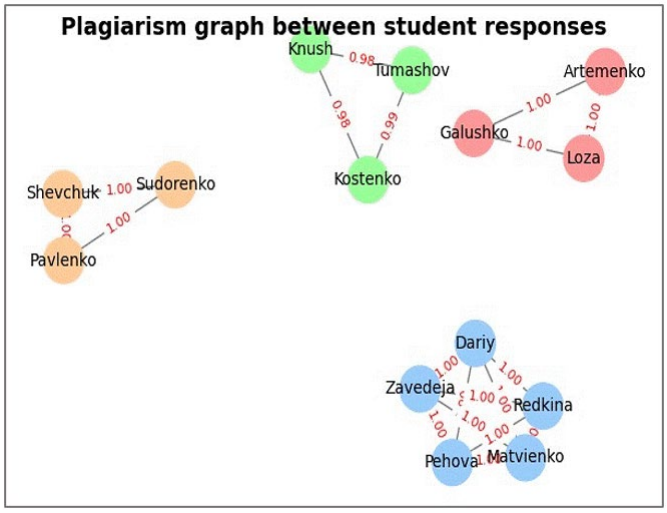


Fig. 8. Visualization of possible plagiarism with similarity coefficients

Compared to traditional methods, the proposed approach allows:

- avoidance of subjective evaluation, including the contrast effect;
- provision of a transparent and reproducible grading logic;
- prompt detection of academic dishonesty, which is more challenging under remote learning conditions.

The educational benefits include:

- reduction in instructor time required to assess large volumes of responses;
- increased objectivity and minimized human bias in grading;
- development of digital competence through the demonstration of modern AI capabilities;
- scalability to different subjects, languages, and types of tasks.

However, certain limitations were identified:

- the quality of evaluation depends on the formulation of the reference answer;
- difficulties arise when working with very short or overly generic responses;
- additional validation is required for integration into official grading systems.

Conclusions

The analysis of scientific publications conducted in the work revealed the need to use artificial intelligence to increase the efficiency of assessing situational tasks in the field of cybersecurity. Given the complexity of assessing students' responses in conditions of distance and blended learning, a new approach was applied, which consists in automated comprehensive assessment of situational tasks taking into account the principle of academic integrity and allows avoiding the contrast effect in assessment. The model created on the basis of Python libraries was tested on a middle-class personal computer, showed stable operation without failures. Processing a large volume of data, (56 responses) took less than 2.5 minutes, which allows for integration into real educational processes without significant resource consumption. The research results confirmed the effectiveness of implementing automated assessment tools for open-ended textual responses to situational tasks in distance and blended learning environments.

The proposed system, based on semantic text analysis, enables:

- a significant reduction in time and effort required for evaluating student responses;
- objective assessment and reduction of the influence of human factors;
- detection of potential cases of academic dishonesty through similarity checks between responses;
- improvement in the overall quality of the educational process due to transparent assessment.

The proposed approach can be scaled and adapted to other disciplines that involve the evaluation of open-ended responses. Future research is planned to:

- enhance the mechanism for generating multiple reference answers;

- implement interpretable explanations for automated scores;
- explore students' reactions to the use of such systems in learning.

Thus, automated assessment becomes an important tool in the digital transformation of education, combining technological efficiency with the need to ensure academic integrity. The application of AI technologies in the form of neural network models for semantic analysis is an effective means of automating assessment processes in education. This ensures the quality, transparency, and scalability of knowledge evaluation, which is especially relevant in distance or blended learning formats.

References:

1. Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks / I. Ievgeniia Kuzminykh et al. *International Journal of Modern Education and Computer Science*. 2021. Vol. 13, no. 6. P. 60–68. URL: https://doi.org/10.5815/ijmecs.2021.06.06.

2. Brandão A., Pedro L., Zagalo N. Teacher professional development for a future with generative artificial intelligence – an integrative literature review. *Digital Education Review*. 2024. No. 45. P. 151–157. URL: https://doi.org/10.1344/der.2024.45.151-157.

3. Gallego-Arrufat M.-J., Torres-Hernández N., Pessoa T. Competence of future teachers in the digital security area. *Comunicar*. 2019. Vol. 27, no. 61. P. 57–67. URL: https://doi.org/10.3916/c61-2019-05.

4. P.A.L. Nadeesha, T.A. Weerasinghe, W.R.N.S Abeyweera. Automatic scoring of knowledge gained and shared through discussion forums: based on the community of inquiry model. *Information Technologies and Learning Tools*. 2025. Vol. 105, no. 1. P. 85–102. URL: https://doi.org/10.33407/itlt.v105i1.5912.

5. Application of artificial intelligence for improving situational training of cybersecurity specialists / Y. V. Shchavinsky et al. *Information Technologies and Learning Tools*. 2023. Vol. 97, no. 5. P. 215–226. URL: https://doi.org/10.33407/itlt.v97i5.5424.

6. Bi X., Shi X., Zhang Z. Cognitive machine learning model for network information safety. *Safety Science*. 2019. Vol. 118. P. 435–441. URL: https://doi.org/10.1016/j.ssci.2019.05.032.

7. The Current Research Status of AI-Based Network Security Situational Awareness / M. Wang et al. *Electronics.* 2023. Vol. 12, no. 10. P. 2309. URL: https://doi.org/10.3390/electronics12102309.

8. AI-Empowered Multimodal Hierarchical Graph-Based Learning for Situation Awareness on Enhancing Disaster Responses / J. Chen et al. *Future Internet*. 2024. Vol. 16, no. 5. P. 161. URL: https://doi.org/10.3390/fi16050161.

9. Burrows S., Gurevych I., Stein B. The Eras and Trends of Automatic Short Answer Grading. International Journal of Artificial Intelligence in Education. 2014. Vol. 25, no. 1. P. 60–117. URL: https://doi.org/10.1007/s40593-014-0026-8.

10. Progress in Neural NLP: Modeling, Learning, and Reasoning / M. Zhou et al. *Engineering.* 2020. Vol. 6, no. 3. P. 275–290. URL: https://doi.org/10.1016/j.eng.2019.12.014.

11. Reimers N., Gurevych I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong*, China. Stroudsburg, PA, USA, 2019. URL: https://doi.org/10.18653/v1/d19-1410.

Автори статті

Легомінова Світлана – доктор економічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-4433-5123

Щавінський Юрій – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-2319-8983

Бударецький Юрій – кандидат технічних наук, старший науковий співробітник, доцент, Національний університет «Львівська політехніка», Львів, Україна.

ORCID: 0000-0001-7208-3827

Будзинський Олександр – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.
ORCID: 0009-0002-2402-0711

Authors of the article

Lehominova Svitlana – Doctor of Sciences (economics), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-4433-5123
Shchavinsky Yuriy – Candidate of Sciences (technical), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0000-0002-2319-8983
Budaretskyi Yuriy – Candidate of Sciences (technical), Senior Researcher, Associate Professor, Lviv Polytechnic National University, Lviv, Ukraine.
ORCID: 0000-0001-7208-3827
Budzynskyi Oleksandr – postgraduate, Department of Cybersecurity and Information Protection, State University of Information and Communication Technologies, Kyiv, Ukraine.
ORCID: 0009-0002-2402-0711