Identification and Prioritization of Risks in the Graduate Thesis Preparation Process Based on a Cognitive Model Formed from Psycholinguistic Experiment Data.

Aleksandr Petrosian
Faculty of Information Technologies
Moscow Polytechnic University
Moscow, Russian Federation
a.a.petrosyan@mospolytech.ru

Ashot Kazarian
Faculty of Information Technologies
Moscow Polytechnic University
Moscow, Russian Federation
kazarian.info@gmail.com

***Abstract*–The article proposes an approach to the diagnosis and prioritization of risks in the process of preparing graduate qualification theses (Thesis) based on a cognitive model. The approach is based on adapting the "attack surface" metaphor from the field of information security to the educational environment, where the thesis preparation process is considered as a system of interconnected components, vulnerabilities, and threats.**

The methodological basis of the study is cognitive modeling of expert representations, reconstructed using psycholinguistic methods. The cognitive model is formed based on data from a directed associative experiment involving academic supervisors from Moscow Polytechnic University specializing in Information Technology and Management.

The obtained empirical data are interpreted in the form of associative networks, which reflect the implicit connections between the components of the thesis preparation process, their vulnerabilities, and possible negative outcomes. A comparative analysis of the cognitive maps of the two expert groups revealed both common and field-specific key problem areas, which attests to the influence of the professional profile on the perception and prioritization of risks in the process of academic supervision.

Keywords–cognitive modeling; psycholinguistics; associative experiment; attack surface; risk management; graduate qualification work (thesis); vulnerabilities of the educational process.

I. INTRODUCTION

The graduate qualification thesis (Thesis) represents the final stage of education, determining the quality of professional training for students at Russian universities. The process of its development is complex and time-consuming, which generates numerous risks at all stages. Traditional management of these risks relies on the experience of academic supervisors and general methodological recommendations, creating a need for formalized tools for systematic risk diagnosis and prioritization.

In the context of education digitalization, the transfer of effective practices from related fields is highly relevant. Educational Data Mining is actively developing, with its primary focuses being academic performance, behavioral characteristics, and student dropout rates [1]. However, the potential of these methods for diagnosing problem areas in processes such as thesis preparation has been realized to a lesser extent [2]. Learning Analytics technologies are promising, but their implementation in higher education practice remains a non-trivial task [3].

As a conceptual framework, the "attack surface" metaphor from information security, which defines the set of vulnerable points in a system, is adapted [4]. A similar network approach is transferred to the educational context. This allows the thesis preparation process to be viewed as a complex system, the individual components of which contain various risk zones. The development of the network approach to the analysis of complex systems has received theoretical justification in [5], and the application of graph neural networks for modeling connections between elements of the educational environment opens new diagnostic possibilities [6]. This approach aligns with the paradigm of integrating risk management into the strategic management of an organization [7]. In this context, the "attack surface" serves as an analytical metaphor for describing potential vulnerabilities at all stages of the work.

Analyzing vulnerabilities requires methods that reveal both explicit and implicit perceptions of risks held by process participants. This task can be addressed through a combination of cognitive modeling and psycholinguistics methods. A special place among them is occupied by the associative experiment, which is aimed at identifying stable verbal and semantic connections in the cognitive representations of experts [8, 9]. The development of students' cognitive abilities, including for knowledge diagnostics, is also facilitated by the use of mind maps [10]. Such approaches are effective for forming and diagnosing cognitive knowledge structures.

The research hypothesis is that combining cognitive modeling and psycholinguistic methods will reveal different risk perception models among academic supervisors from different professional backgrounds. It is expected that the cognitive risk map will differ between instructors from technical and management profiles. This difference is attributed to the specifics of their professional thinking and experience. The

consequence is different approaches to risk assessment, which directly affects managerial decisions during thesis supervision.

Thus, the key task becomes the development of an analytical approach for structuring the risks of the thesis preparation process and empirically identifying their priority. This approach is based on the concept of risks as outcomes of the interaction between components, their vulnerabilities, and undesirable consequences. This concept is formalized in the form of an "attack surface" model.

Research objective: development and approbation of a method for cognitive risk diagnostics in the thesis preparation process.

To achieve this objective, the following tasks were set:

1. To formalize the "attack surface" model for the educational process of thesis preparation.
2. To collect expert data on risk perception using a directed associative experiment with two profile groups of academic supervisors.
3. To analyze the structure of associative connections, construct and compare cognitive maps to identify key vulnerabilities and their priorities in each group.

Scientific novelty of the research lies in the synthesis of the "attack surface" concept from information security and the psycholinguistic method of the directed associative experiment to solve the problem of diagnosing educational risks. This allows not only to formalize the risk system of thesis preparation in the form of a model but also to empirically reconstruct the implicit cognitive structures of their perception by different professional groups of experts.

II. THEORETICAL MODEL

The research is based on a cognitive model of risks in the thesis writing process, which formalizes the key entities and the relationships between them. The model integrates an ontological description of the process with a graph representation of a cognitive map and operates with three basic sets.

Set C (Components) includes the key components of the thesis preparation and defense process, understood as functional nodes uniting participants, resources, content elements, and control stages::

- C1. Student;
- C2. Academic Supervisor;
- C3. Thesis Topic;
- C4. Research Methodology;
- C5. Material and Technical Resources;
- C6. Work Organization;
- C7. Thesis Content and Results;
- C8. Pre-defense and Review;
- C9. Defense Procedure;
- C10. Regulatory and Methodological Environment.

Set V (Vulnerabilities) represents typical vulnerabilities – functional and cognitively perceived states of components that increase the probability of undesirable outcomes:

- V1. Low motivation (C1);
- V2. Lack of basic knowledge and skills (C1);
- V3. Procrastination and ineffective time management (C1);
- V4. Limited time resources of the supervisor (C2);
- V5. Lack of expert experience (C2);
- V6. Insufficient elaboration of the topic selection stage (C3);
- V7. Insufficient specification of the goal and objectives (C3);
- V8. Inaccuracies in the choice of methodology (C4);
- V9. Lack of necessary resources (C5);
- V10. Technical failures and limitations (C5);
- V11. Inaccuracies in stage planning (C6);
- V12. Insufficient quality of the work (C7);
- V13. Non-compliance with formal requirements (C7, C10);
- V14. Formal attitude towards the pre-defense (C8);
- V15. Formal reviewer's report (C8);
- V16. Insufficient preparation for the defense (C9).

Set A (Attacks) defines the main undesirable outcomes (realized risks):

- A1. Low quality of the thesis;
- A2. Unsuccessful defense;
- A3. Missed deadlines;
- A4. Conflict situation between participants;
- A5. Violations of academic integrity;
- A6. Failure to achieve research objectives.

The conceptual model represents a three-level "Component – Vulnerability – Attack" (C-V-A) structure. Its elements are connected by directed relations: $C \rightarrow V$ describes the emergence of vulnerabilities in components, and $V \rightarrow A$ describes the realization of undesirable outcomes. The model also takes into account direct implicit associations $C \rightarrow A$, reflecting stable cognitive connections in the minds of experts, and serves as a basis for risk analysis and prioritization.

The "Attack Surface" zone [11] is represented as a subset of key model elements (C-V-A) possessing the greatest centrality in the weighted associative graph constructed from expert responses. Identifying this zone based on network metrics

allows the transition from risk description to risk prioritization. The elements of the "attack surface" indicate priority directions for managerial intervention.

Contemporary research [12] in the field of Learning Analytics emphasizes the importance of creating informative analytical systems to support the educational process. The application of knowledge graphs for structuring and teaching academic disciplines opens new opportunities in education [13].

The developed model served as the conceptual foundation for forming the stimulus material of the associative experiment.

III. CONDUCTING THE ASSOCIATIVE EXPERIMENT

The purpose of the experiment is to empirically verify the applicability of the theoretical model and to identify how its elements correlate in the cognitive representations of experts from different professional profiles. A directed associative experiment was chosen as the diagnostic tool. Unlike traditional surveys, this method captures stable connections at the level of automated cognitive perception. This is particularly significant for studying hidden mental structures [14, 15]. In this study, the choice of method is determined by its ability to reveal the professional experience and established perceptions of academic supervisors. The elements of the Component set C were used as the basis for forming the stimuli. Each of the 10 components was reduced to a generalized stimulus word reflecting its semantic content. On this basis, the stimulus set S was defined, including the following elements:

- S1. "Student";
- S2. "Supervisor";
- S3. "Topic";
- S4. "Method";
- S5. "Resources";
- S6. "Plan";
- S7. "Results";
- S8. "Review";
- S9. "Defense";
- S10. "Requirements".

Associative reactions to these stimuli were considered as indicators of the connection between a component and vulnerabilities (V) or directly with negative outcomes (A).

The experiment was conducted individually in a face-to-face format. The researcher read the instructions and presented the stimuli, recording the experts' responses in an electronic spreadsheet. The experiment had a directed nature: it was explained to respondents that their associations should relate to risks and problematic situations in thesis preparation from the perspective of the academic supervisor.

For each verbally presented stimulus, the participant gave one mandatory verbal reaction – the first word or short phrase that came to mind. The maximum number of reactions was limited to three. The instructions were aimed at capturing the most involuntary, stable cognitive connections reflecting real experience.

All 10 stimuli were presented to each respondent in a unique random order, which made it possible to neutralize the sequence effect. Each stimulus was presented only once.

The study involved 8 instructors from Moscow Polytechnic University who supervise graduate theses. Two expert groups of 4 people each were formed: instructors from the Faculty of Information Technologies (IT group) and instructors from the Faculty of Management and Economics (Management group). The average work experience in education for the IT group was 9.75 years, and for the Management group – 13.75 years. The overall average experience of the experts was 11.75 years, with a minimum threshold of 5 years, which guarantees the necessary level of expertise and familiarity with the typical risks of the process.

The sample of respondents includes experienced supervisors from two different profile areas to compare their cognitive risk maps.

IV. DATA PROCESSING AND ANALYSIS

The processing of the obtained data included three main stages:

1. Normalization of reactions and data clustering.
2. Construction of adjacency matrices and calculation of metrics.
3. Generation of the associative network and performance of network analysis.

At the data collection stage, a high relevance of the selected stimuli to the theoretical model was noted. Many associative reactions confirmed the expected connections. For example, in response to stimulus S1 "Student", words characterizing vulnerabilities were often encountered: "lazy", "disorganized", which corresponds to categories V1 (low motivation) and V2 (lack of skills). Similarly, stimulus S6 "Plan" elicited reactions such as "falling behind" and "missing deadlines", which reflects the negative scenario A3 (missed deadlines). These observations confirmed the content validity of the stimulus material and formed the basis for further processing.

The obtained verbal reactions were subjected to a semantic normalization procedure. For this purpose, synonymous expressions were reduced to generalized concepts corresponding to the elements of sets V and A. Due to the wide variety of reactions and spelling variants, a locally deployed large language model, Qwen2.5 7B Instruct, built on a transformer architecture, was used for primary automated clustering. To optimize computational efficiency while preserving semantic accuracy, the model was quantized using the Q6_0 GGUF method. To improve accuracy and account for the context of professional activity, the clustering results were additionally verified and corrected manually by the researcher.

Automated clustering followed by expert validation made it possible to form an aggregated associative field for each group and reliably assign each reaction to a specific vulnerability or attack. Based on the normalized data, clusters were identified

and the number of reactions assigned to each category was counted. The obtained frequency indicators formed the basis for calculating quantitative metrics and constructing an adjacency matrix, where the strength of the connection between a stimulus (component) and a concept (vulnerability/attack) was determined by the frequency of corresponding associations. This matrix became the foundation for visualizing the cognitive map in the form of a weighted graph.

The use of graphs for knowledge representation aligns with modern approaches to modeling complex systems and data analysis [16], where the key object of study is the identification and analysis of connections between entities. This representation format opens prospects for applying network analysis algorithms and machine learning methods that work with graph structures [17]. The cognitive validity of the approach is confirmed by its correspondence to classical models of semantic memory organization [18], in which knowledge is represented as networks of related concepts.

After performing normalization and clustering of the verbal reactions obtained from both groups of respondents, the data were presented in the form of an adjacency matrix. It reflects the degree of connectivity between stimuli (S) and the obtained reactions (R) in the collective consciousness of academic supervisors. The stimuli (S) reflect the set of components (C), and the reactions (R) reflect the sets of vulnerabilities (V) and attacks (A). This approach made it possible to identify the representation of the real C-V-A model in the consciousness of each respondent group, as well as to aggregate the data into a general model.

To ensure clarity and perform a comparative analysis of the models, the absolute values were converted into relative ones. Thus, for each obtained association related to a vulnerability (V) or attack (A), 12.5% was added to the connection weight, which corresponded to the total number of participants (8 people). This made it possible to assess the contribution of each vulnerability and attack in the collective consciousness of the respondents. Table 1 presents the aggregated data, reflecting the strength of connections as percentages in the C-V-A model based on the reactions obtained from both groups of academic supervisors.

Table 1

Aggregated Adjacency Matrix (%)

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
V1	62.5									
V2	75									
V3	87.5									
V4		50								
V5		25								
V6			50							
V7			25							
V8				62.5						
V9					62.5					
V10					37.5					
V11						50				
V12							50			
V13							37.5			25
V14								37.5		
V15								25		
V16									37.5	
A1								37.5		
A2							37.5			
A3	75									
A4	12.5	12.5								
A5	12.5		25							
A6							12.5			

The resulting table reflects the degree of connection between the set of components (C) and the sets of vulnerabilities (V) and attacks (A), which creates the basis for further construction of graph models. To assess each vulnerability (V) and attack (A), significance metrics were calculated based on the frequency of their mention in the associative fields for each expert group. The degree of importance of a concept was defined as the proportion of respondents in the group who gave at least one association attributed to that concept. Formally, for each concept *k* from sets V and A, the metrics were calculated using formulas (1) – (3):

$$Sum_{IT_k} = \left(\frac{N_{IT_k}}{N_{IT}}\right) * 100\%, \text{where } k \in V \text{ or } k \in A \quad (1)$$

$$Sum_{Management_k} = \left(\frac{n_{Management_k}}{N_{Management}}\right) * 100\% \quad (2)$$

$$Sum_{Total_k} = \left(\frac{(n_{IT} + n_{Management})}{(N_{IT} + N_{Management})}\right) * 100\% \quad (3)$$

where:

- N_{IT_k} and $N_{Management_k}$ are the number of respondents in the "IT" and "Management" groups, respectively, whose associations were attributed to concept *k*;
- $N_{IT} = N_{Management} = 4$ (Number of respondents in each group);
- $N_{IT} + N_{Management} = 8$ (Total number of respondents).

For clarity, the obtained results are presented in Table 2. Within each group, the contribution of an individual association to the strength of connection between concepts was $\frac{1}{4} = 25\%$, and in the aggregated model $\frac{1}{8} = 12.5\%$. The obtained data were sorted by the SumTotal metric, which allows identifying the most significant vulnerabilities (V) and attacks (A).

Table 2

Identification of the Most Significant Vulnerabilities and Attacks.

Concept	Sum_IT	Sum_Management	Sum_Total
V3	75%	100%	87.50%
A3	75%	75%	75%

V2	75%	75%	75%
V1	50%	75%	62.50%
V13	50%	75%	62.50%
V9	75%	50%	62.50%
V8	75%	50%	62.50%
V11	50%	50%	50%
V4	50%	50%	50%
V6	75%	25%	50%
V12	50%	50%	50%
A1	50%	25%	37.50%
A2	25%	50%	37.50%
A5	50%	25%	37.50%
V14	25%	50%	37.50%
V16	25%	50%	37.50%
V10	75%	0%	37.50%
V5	25%	25%	25%
V7	25%	25%	25%
V15	25%	25%	25%
A6	25%	0%	12.50%
A4	0%	25%	12.50%

For a visual representation, the data were transformed into a graphical form, presented in Figure 1.

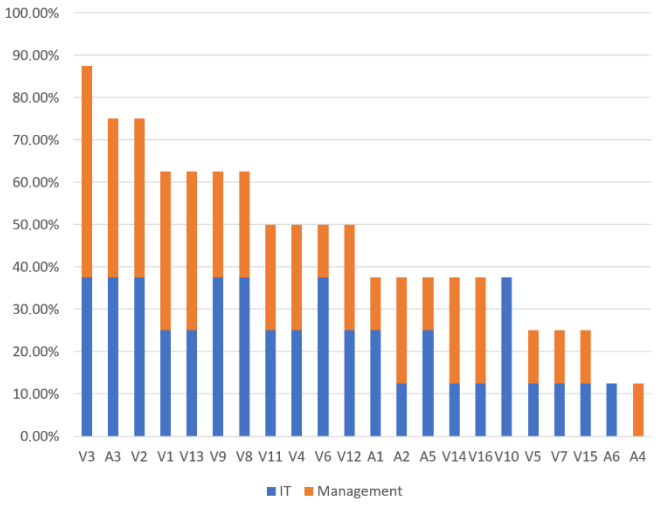

Figure 1. Prioritization of vulnerabilities (V) and attacks (A) for each respondent group.

To visualize the obtained data and create a cognitive model, an associative network was constructed, which allowed for its comparative analysis. During the visualization process, to ensure the interpretability of the results, principles for enhancing the cognitive clarity of graph models [19] were applied, such as minimizing edge crossings and visually encoding the strength of connections (edge thickness). The analysis of associative reactions to these stimuli revealed stable connections between the elements of sets C, V, and A.

The associative network reflects the stable connections established in the respondents' consciousness regarding the topic of vulnerabilities and risks in the thesis writing process. It takes the form of weighted directed graphs, which were created using specialized software Gephi. The final graph, including reactions from both groups of respondents, is presented in Figure 2.

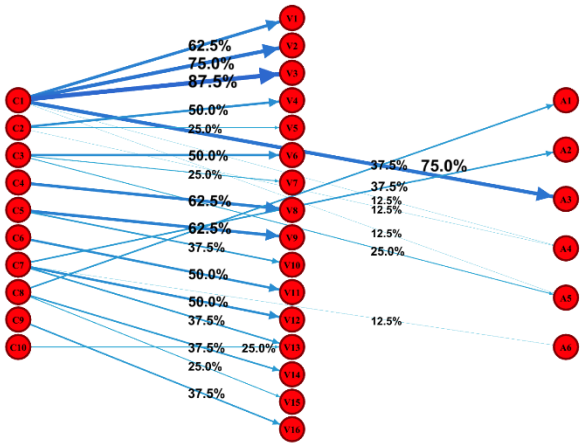

Figure 2. Aggregated associative network of both supervisor groups.

The nodes of the graph were the original stimulus words, representing the key components (C), vulnerabilities (V), and attacks (A) of the thesis writing process. An edge between two nodes was drawn if at least one associative connection existed between these concepts within the group's associative field. The weight of the edge $w(C, V)$ or $w(C, A)$ was determined by the total frequency of such common associations, which quantitatively reflected the strength of the semantic connection between concepts. In the visual representation of the graph, this weight is reflected as the thickness of the corresponding edge.

Separate cognitive graphs were constructed for each group in a similar manner. To perform network analysis and compare the two models, the Weighted Degree Centrality (WDC) metric was used, calculated by formula (4):

$$WDC(i) = \sum_{j} w(i,j) \quad (4)$$

This metric, serving as a standard tool for analyzing the significance of vertices in networks, is effectively applied to identify the modular structure of communities in risk diagnostics [20] and quantitatively reflects the significance of a node in the network: the more strong connections a concept has with other concepts, the higher its centrality. In the visual representation of the graph, the value of this metric is projected onto the node size. Nodes with the highest weighted degree centrality are interpreted as key problem areas in the perception of risks by experts of the corresponding group. Stimulus nodes with the highest weighted degree centrality values were identified as the

key elements of the cognitive risk map, forming the “attack surface” for each group.

V. RESULTS OF THE STUDY

Analysis of the aggregated data (Table 2) showed that three risks dominate the general perception model of all experts: procrastination (V3 – 87.5%), missed deadlines (A3 – 75%), and students' lack of basic knowledge (V2 – 75%).

Examination of the perception structure by groups (Figure 1) revealed profile-specific characteristics. The diagram clearly shows the dominance of IT specialists (blue segments) in the categories of methodology and resources, while managers (orange segments) exhibit predominantly indicators related to the human factor. For supervisors from the IT field, the focus is on methodology and resources: vulnerabilities V8 (methodological inaccuracies), V9 (lack of resources), and V10 (technical failures) each scored 75% (with V10 being completely absent in the Management group). Topic elaboration (V6 – 75%) is also significant. In the Management group, priorities are shifted towards the human factor: maximum values are observed for V3 (procrastination – 100%), V1 (low motivation – 75%), V2 (lack of knowledge – 75%), and V13 (non-compliance with requirements – 75%).

Comparative analysis confirms the hypothesis regarding the influence of professional profile on risk perception. However, both groups are united in identifying a universal critical point – the threat of missed deadlines (A3 – 75% in both groups), closely associated with student procrastination (V3).

Based on the identified “attack surface”, differentiated measures are proposed. To counteract the universal threat of missed deadlines, the implementation of digital progress trackers is advisable. For the IT field, methodological guidelines and resource audits are relevant; for the management profile, interim motivational interviews and monitoring of requirement compliance are recommended.

VI. CONCLUSION

This study has implemented and tested a method for diagnosing risks in the preparation of graduate qualification theses, based on a synthesis of the “attack surface” metaphor from the field of information security and methods of cognitive psycholinguistics.

The main result is the approbation of a risk diagnostics method founded on the synthesis of the “attack surface” concept and psycholinguistic tools. The cognitive model (C-V-A) has confirmed its effectiveness as a conceptual framework for forming stimuli and interpreting data. The method of the directed associative experiment, followed by the construction and comparison of associative networks, made it possible to identify and visually compare the key problem areas in the perception of experts from two different profiles. Pronounced differences in risk priorities were established, and a universal critical element – the problem of meeting deadlines – was also identified.

The existence of significant differences in risk perception between academic supervisors from technical and management profiles has been experimentally proven, which confirms the influence of the professional belief system on threat assessment. At the same time, a universal critical element of the “attack surface” was identified – the threat of missed deadlines (A3), closely linked in the experts' consciousness to the vulnerability of student procrastination (V3). This identifies the development of self-organization and time management skills in students (C1) as a priority direction for managerial intervention.

The practical significance of the work lies in the creation of a toolkit for differentiated and proactive risk management, enabling the formulation of targeted recommendations for various levels of the educational system. The developed method aligns with the principles of structured and adaptive risk management defined in the international standard ISO 31000:2018, according to which the process should be iterative, consider the internal and external context of the organization, and ensure continuous improvement based on data analysis [21].

The development of the proposed approach corresponds to current trends in the integration of psycholinguistics and computational linguistics methods. As demonstrated in study [22], the analysis of associative word characteristics in combination with sentiment analysis methods allows not only for the identification of hidden emotional connections but also for a significant improvement in the quality of textual data interpretation. The application of such combined methods opens additional opportunities for in-depth analysis of cognitive maps reconstructed during associative experiments and increases the reliability of diagnosing emotionally charged risk zones in the educational process.

VII. REFERENCES

[1] N. A. Popova and E. S. Egorova, “Osnovnye napravleniya intellektual'nogo analiza dannykh v sfere obrazovaniya [Main directions of educational data mining],” (in Russian), Izvestiya Kabardino-Balkarskogo nauchnogo tsentra RAN, vol. 26, no. 5, pp. 94–106, 2024, doi: 10.35330/1991-6639-2024-26-5-94-106.

[2] I. Papadogiannis, V. Poulopoulos, and M. Wallace, “A critical review of data mining for education: What has been done, what has been learnt and what remains to be seen,” International Journal of Educational Research Review, vol. 5, no. 4, pp. 353–372, 2020, doi: 10.24331/ijere.75504.

[3] L. Šereš, V. Pavlićević, G. Petrović, D. Horvat, and R. Ivanišević, “Learning analytics: prospects and challenges,” Strategic Management, vol. 27, no. 2, 2022, doi: 10.5937/StraMan2200020S.

[4] A.-L. Barabási, Network Science. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[5] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Liò, and Y. Bengio, “Graph Attention Networks,” in Proc. Int. Conf. Learn. Represent. (ICLR), 2017. doi: 10.48550/arXiv.1710.10903.

[6] P. Chen, Y. Lu, V. W. Zheng, X. Chen, and B. Yang, “KnowEdu: A system to construct knowledge graph for education,” IEEE Access, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2839607.

[7] F. Mizrak, “Integrating cybersecurity risk management into strategic management: a comprehensive literature review,” Research Journal of Business and Management, vol. 10, no. 3, pp. 98–108, 2023, doi: 10.17261/Pressacademia.2023.1807.

[8] A. Petrosian and A. Philippovich, “Assessing the knowledge of students in the field of computer networks using associative experiments,” in 2025 Int. Russian Smart Ind. Conf. (SmartIndustryCon), Sochi, Russian Federation, 2025, doi: 10.1109/SmartIndustryCon65166.2025.10986104.

[9] N. I. Konovalova, "'Russian Associative Dictionary' as a source of information about metalanguage consciousness in verbal memory of speakers," in Advances in Social Science, Education and Humanities Research, vol. 437, pp. 399–403, 2020.

[10] O. Yu. Muller, "Primenenie mental'nykh kart v razvitii kognitivnykh sposobnostey studentov [The use of mind maps in the development of students' cognitive abilities]," (in Russian), Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo. Seriya: Sotsial'nye nauki, no. 3 (70), pp. 206–211, 2023, doi: 10.52452/18115942_2023_3_206.

[11] M. Atighetchi, B. Simidchieva, F. Yaman, T. Eskridge, M. Carvalho, and N. Paltzer, "Using ontologies to quantify attack surfaces," in Proc. Int. Conf. Semantic Technol. Intell., Defense, Security (STIDS), 2016, pp. 10–18.

[12] H. Drachsler, Towards Highly Informative Learning Analytics. Heerlen, The Netherlands: Open Universiteit, 2023.

[13] E. Ilkou, H. Abu-Rasheed, D. Chaves-Fraga, E. Engelbrecht, E. Jiménez-Ruiz, and J. E. Labra-Gayo, "Teaching knowledge graph for knowledge graphs education," Semantic Web, 2025. (In Press)

[14] O. Viberg, I. Jivet, and M. Scheffel, "Designing culturally aware learning analytics: A value sensitive perspective," in Practicable Learning Analytics, O. Viberg and Å. Grönlund, Eds. Springer Nature, 2022. doi: 10.48550/arXiv.2212.09645.

[15] P. V. Men'shikov, "Assotsiativnyy eksperiment v izuchenii sistemy predstavleniy obuchayemogo o didakticheskoy kommunikatsii [Associative experiment in studying the system of student's ideas about didactic communication]," (in Russian), Vestnik Omskogo gosudarstvennogo pedagogicheskogo universiteta. Gumanitarnye issledovaniya, no. 2, pp. 174–179, 2023.

[16] M. A. Anik'eva, "Primenenie grafov znaniy v obrazovatel'noy srede dlya personalizirovannogo obucheniya [The use of knowledge graphs in the educational environment for personalized learning]," (in Russian), Informatika i obrazovanie, vol. 36, no. 10, pp. 33–42, 2021, doi: 10.32517/0234-0453-2021-36-10-33-42.

[17] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 4–24, Jan. 2021, doi: 10.48550/arXiv.1901.00596.

[18] A. M. Collins and E. F. Loftus, "A spreading-activation theory of semantic processing," Psychol. Rev., vol. 82, no. 6, pp. 407–428, Nov. 1975, doi: 10.1037//0033-295X.82.6.407.

[19] M. E. J. Newman, "Modularity and community structure in networks," Proc. Nat. Acad. Sci. USA, vol. 103, no. 23, pp. 8577–8582, Jun. 2006, doi: 10.1073/pnas.0601602103.

[20] R. A. Isaev and A. G. Podvesovskiy, "Povyshenie kognitivnoy yasnosti grafovykh modeley predstavleniya znaniy i prinyatiya resheniy s primeneniem vizualizatsii [Improving cognitive clarity of graph models for knowledge representation and decision-making using visualization]," (in Russian), Ergodizayn, no. 1 (11), 2021.

[21] Risk management – Guidelines, ISO Standard 31000:2018, 2018.

[22] A. Y. Philippovich and V. S. Lukyanenko, "Analysis of associative and sentimental characteristics of words for revealing hidden emotions and correlations," in 2025 Int. Russian Smart Ind. Conf. (SmartIndustryCon), Sochi, Russian Federation, 2025, doi: 10.1109/SmartIndustryCon65166.2025.10986282.