МРНТИ 20.23.21 **https://doi.org/10.58805/kazutb.v.4.29-1285**

МОДЕЛИРОВАНИЕ СЦЕНАРИЕВ НАРУШЕНИЙ ЦЕЛОСТНОСТИ ДАННЫХ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ КОММУНИКАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

[1]Л.О. Жумабаева, [2]Mohamed Othman, [1]М.А. Орынбасар, [1]Б.А. Жұмажан, [1]М.Е. Ақбердиева
[1]Каспийский университет технологий и инжиниринга имени Ш. Есенова, г. Актау, Казахстан
[2]Universiti Putra Malaysia, Malaysia

Корреспондент-автор: maksym1.orynbassar@yu.edu.kz

В статье рассматриваются интеллектуальные социальные системы (ИСС) представляют собой интегрированные цифровые экосистемы, объединяющие пользователей, аналитические сервисы и алгоритмы искусственного интеллекта для управления коммуникациями, репутационными процессами и общественным взаимодействием. К таким системам относятся социальные сети, государственные платформы цифрового взаимодействия («Госуслуги», «Активный гражданин»), краудсорсинговые площадки и образовательные онлайн-экосистемы.

Главная особенность ИСС заключается в их высокой социальной значимости данных. Ошибки, подмены или целенаправленные манипуляции в информационных потоках ведут не только к технологическим, но и к социальным последствиям — снижению уровня доверия пользователей, распространению дезинформации, искажению общественного мнения и результатов электронных голосований.Таким образом, обеспечение целостности данных в ИСС становится одной из ключевых задач цифрового общества. Необходимо не только защитить данные от внешних воздействий, но и гарантировать корректность, достоверность и непротиворечивость их формирования, хранения и обработки.

Ключевые слова: интеллектуальные социальные системы, имитационное моделирование, целостность данных, когнитивные атаки, информационные искажения, агентное моделирование, машинное обучение, нейросетевые алгоритмы, графовые нейронные сети, автоэнкодеры, LSTM, цифровое доверие, поведенческие аномалии, анализ информационных потоков, обеспечение безопасности данных.

ИНТЕЛЛЕКТУАЛДЫ КОММУНИКАЦИЯЛЫҚ ӨЗАРА ӘРЕКЕТТЕСУ ЖҮЙЕЛЕРІНДЕГІ ДЕРЕКТЕР ТҰТАСТЫҒЫНЫҢ БҰЗЫЛУ СЦЕНАРИЙЛЕРІН МОДЕЛЬДЕУ

[1]Л.О. Жумабаева, [2]Mohamed Othman, [1]М.А. Орынбасар, [1]Б.А. Жұмажан, [1]М.Е. Ақбердиева
[1]Ш.Ш. атындағы Каспий технологиялар және инжиниринг университеті. Есенов, г. Актау, Казахстан,
[2]Universiti Putra Malaysia, Malaysia,
e-mail: maksym1.orynbassar@yu.edu.kz

Мақалада интеллектуалды әлеуметтік жүйелер (ИАЖ) интеграцияланған цифрлық экожүйелер ретінде қарастырылады, олар пайдаланушыларды, талдамалық сервистерді және жасанды интеллект алгоритмдерін біріктіріп, коммуникацияларды, беделдік процестерді және қоғамдық өзара іс-қимылды басқаруға мүмкіндік береді. Мұндай жүйелерге әлеуметтік желілер, цифрлық өзара әрекеттесу мемлекеттік платформалары («Электрондық үкімет», «Белсенді азамат»), краудсорсинг алаңдары және онлайн-білім беру экожүйелері жатады.ИАЖ-дың негізгі ерекшелігі – деректердің жоғары әлеуметтік маңыздылығы. Ақпараттық ағындардағы қателіктер, алмастырулар немесе әдейі жасалған манипуляциялар тек технологиялық емес, сонымен қатар әлеуметтік салдарға әкеледі — пайдаланушылар сенімінің төмендеуі, дезинформацияның таралуы, қоғамдық пікір мен электрондық дауыс беру нәтижелерінің бұрмалануы.

Сондықтан деректердің тұтастығын қамтамасыз ету цифрлық қоғамның негізгі міндеттерінің бірі болып табылады. Деректерді сыртқы әсерлерден қорғап қана қоймай, олардың қалыптасуының, сақталуының және өңделуінің дұрыстығын, сенімділігін және қайшылықсыздығын қамтамасыз ету қажет.

Түйін сөздер: интеллектуалды әлеуметтік жүйелер, имитациялық модельдеу, деректердің тұтастығы, когнитивтік шабуылдар, ақпараттық бұрмалау, агенттік модельдеу, машиналық оқыту, нейрожелілік алгоритмдер, графтық нейрондық желілер, автоэнкодерлер, LSTM, цифрлық сенім, мінез-құлық аномалиялары, ақпараттық ағындарды талдау, деректер қауіпсіздігін қамтамасыз ету.

MODELING SCENARIOS OF DATA INTEGRITY VIOLATIONS IN INTELLIGENT COMMUNICATIVE INTERACTION SYSTEMS

[1]L.O. Zhumabayeva, [2]Mohamed Othman, [1]M.A. Orynbassar, [1]B.A. Zhumazhan, [1]M.E. Akberdiyeva

[1]Sh. Yessenov Caspian University of Technology and Engineering, Aktau, Kazakhstan,
[2]Universiti Putra Malaysia, Malaysia,
e-mail: maksym1,orynbassar@yu.edu.kz

The article is examined intelligent social systems (ISS) as integrated digital ecosystems that unite users, analytical services, and artificial intelligence algorithms to manage communications, reputation processes, and public interaction. Such systems include social networks, government digital interaction platforms (“Gosuslugi”, “Active Citizen”), crowdsourcing platforms, and educational online ecosystems. The main feature of ISS lies in the high social significance of their data. Errors, substitutions, or deliberate manipulations in information flows lead not only to technological but also to social consequences — reducing user trust, spreading disinformation, and distorting public opinion and electronic voting results.

Thus, ensuring data integrity in ISS becomes one of the key challenges of the digital society. It is necessary not only to protect data from external influences but also to guarantee the correctness, reliability, and consistency of their formation, storage, and processing.

Keywords: intelligent social systems, simulation modeling, data integrity, cognitive attacks, information distortion, agent-based modeling, machine learning, neural network algorithms, graph neural networks, autoencoders, LSTM, digital trust, behavioral anomalies, information flow analysis, data security assurance.

Introduction. The modern information space is characterized by a high degree of interconnectedness, rapid data exchange, and the widespread implementation of artificial intelligence (AI) technologies in social and managerial processes. Against this backdrop, a special role is played by intelligent social systems (ISS) - integrated digital ecosystems that bring together users, analytical services, and AI algorithms to manage communication, reputation processes, and public interaction. Such systems include social networks, government digital interaction platforms (e.g., “Gosuslugi”, “Active Citizen”), crowdsourcing platforms, and online educational ecosystems, in which vast volumes of user data continuously circulate.

In the context of the digital transformation of society, data become a strategic resource that determines the effectiveness of decision-making, the level of trust in digital platforms, and the resilience of social infrastructure. Violations of data integrity - whether caused by technical failures, deliberate manipulations, or cognitive distortions - have a significant impact on the reliability of information, undermine the reputation of digital services, and can lead to the destabilization of social processes.

Data integrity in intelligent systems is not limited to preservation and immutability; it also includes ensuring semantic, behavioral, and temporal consistency. Traditional protection methods based on cryptographic approaches (hashing, digital signatures, backup mechanisms) are proving insufficient under current conditions. They do not take into account the socio-cognitive aspects of digital interaction, where the source of distortion may be the behavior of users themselves, of algorithms, or of bots.

In this regard, the development of intelligent methods for analysis and modeling capable of detecting hidden threats and forecasting scenarios of data degradation in ISS becomes an urgent

scientific challenge. One of the most promising approaches to addressing this problem is simulation modeling, which makes it possible to reproduce complex socio-informational processes, investigate the dynamics of data integrity violations, and assess the impact of various factors on their propagation.

Simulation modeling, when combined with machine learning methods and neural network analysis, enables the creation of experimental digital twins of social systems, where the patterns of cognitive attacks, fake activity, and other forms of anomalies can be studied. This opens up new prospects for building digital trust systems in which intelligent algorithms perform functions of diagnostics, adaptation, and restoration of data integrity in real time.

Thus, this study is aimed at developing a methodology for simulation modeling of data integrity violations in intelligent social systems and at creating analytical tools capable of enhancing the reliability and resilience of digital ecosystems.

Literature Review. The problem of ensuring data integrity in intelligent social systems (ISS) is one of the key topics in contemporary digital science. In recent years, interest has grown significantly in studying the relationship between the technical and social aspects of ISS functioning, where data violations are considered not only as the result of cyberattacks, but also as a consequence of cognitive biases, user behavior, and algorithmic anomalies. Modern researchers note that intelligent social systems represent complex human–machine ecosystems in which information flows are formed simultaneously at the technological and behavioral levels. Therefore, classical information protection methods based solely on cryptographic principles are becoming insufficient. There is a need for comprehensive approaches that combine simulation modeling, machine learning, and behavioral analysis.

According to studies in the field of digital security, data integrity violations in ISS often have a systemic character: an error or distortion at one level leads to cascading consequences in other subsystems. This requires constructing models that take into account the dynamics of interrelations and the behavior of agents within the network. Under such conditions, simulation models make it possible to forecast scenarios of data degradation and to assess the system's resilience to external and internal threats [1].

The works of foreign authors highlight the effectiveness of agent-based modeling (ABM) for analyzing social interactions and the spread of informational distortions [2]. Models based on graph neural networks (GNN) make it possible to identify structural dependencies and detect anomalies in users' network activity. In addition, domestic researchers emphasize the role of learning analytics and digital trust in the design of ISS. Maintaining data integrity in educational and social ecosystems requires diagnostic and adaptive tools that are capable not only of recording violations but also of preventing them through intelligent self-learning mechanisms of the system.

A physiological analogue of such processes can be found in the adaptation of living systems to stress conditions, where the system, when facing external influences, develops resilience and compensation mechanisms [3]. Similarly, intelligent social systems must possess the property of digital resilience that allows them to preserve the reliability and consistency of data in the face of failures and information attacks.

In recent years, special attention has been paid to cognitive attacks and informational distortions arising from manipulations in digital communication processes [4]. These phenomena require a comprehensive analysis that integrates psychological, technical, and behavioral aspects. The use of simulation models makes it possible to reproduce the process of false information dissemination and to evaluate the effectiveness of detection algorithms.

Based on the literature analysis, several key research directions in the field of data integrity modeling can be distinguished:

- development of multi-level modeling architectures that integrate technical and cognitive components;

- application of machine learning and neural

networks for the analysis of network interactions and anomalies;

- investigation of digital trust models and ethical principles of ISS functioning;

- implementation of simulation models for diagnosing and forecasting data integrity violations in real time.

Thus, the literature review shows that simulation modeling of data integrity violations is a relevant research area that integrates interdisciplinary approaches from artificial intelligence, cybersecurity, learning analytics, and socio-technical design. The development of such models contributes to the formation of intelligent digital trust systems, which is of strategic importance for the digital transformation of society.

Materials and methods. To test the hypothesis regarding the possibility of predicting and detecting data integrity violations in intelligent social systems (ISS), a comprehensive experiment was conducted based on simulation modeling and machine learning methods. The study included several stages: model design, computational experiments, and analysis of the results.

The methodological framework of the study was based on the principle of three-level modeling, which involves decomposing the system into interrelated levels: user, informational, and infrastructural. At the user level, the behavior of agents was modeled to imitate user interactions in social networks, government digital services, and crowdsourcing platforms. The informational level reflected the dynamics of data flows, their transmission, transformation, and potential distortions under the influence of external and cognitive factors. The infrastructural level included network connections, server nodes, and communication channels that ensure storage, processing, and synchronization of information.

The simulation model was implemented using the AnyLogic software environment and Python (SimPy and Pandas libraries). This made it possible to combine visual modeling with analytical calculation of indicators and statistical data processing. At the first stage, agent-based scenarios of user interaction were created, with different levels of activity, degrees of trust in information sources, and probabilities of spreading distorted information.

To assess system resilience and data integrity, the following computational indicators were used: Integrity Rate, Distortion Propagation Factor, Resilience Index, and Entropy Shift of the information space. These parameters made it possible to quantitatively measure system stability under the influence of various risk factors and cognitive attacks.

Two experimental models were used in the study. The control model reflected the traditional architecture of ISS without intelligent data recovery mechanisms, while the experimental version included machine learning algorithms capable of automatically detecting anomalies and restoring distorted data. Deep learning methods were applied for analysis: autoencoders, recurrent neural networks (LSTM), and graph neural networks (GNN). Autoencoders were used to detect behavioral anomalies, LSTM networks to analyze temporal dependencies in data flows, and GNN models to study network structures and relationships between nodes.

In the course of the computational experiment, 10,000 virtual agents interacting over 1,000 discrete time steps were simulated. Each agent was characterized by individual parameters: level of trust, activity frequency, propensity to spread information, and threshold of critical perception [5].

The results of the experiment showed that, in the control model, the level of data integrity decreased on average by 28% under the influence of external cognitive attacks and fake messages [6]. In the experimental model equipped with self-learning mechanisms, the Integrity Rate remained stable and decreased by no more than 7-10%, which indicates the high effectiveness of the proposed approach.

A correlation analysis was also carried out between the structure of social ties and the probability of data distortion. It was found that a high density of links in local clusters accelerates the

spread of distortions; however, the application of adaptive trust algorithms and content filtering can significantly reduce this effect.

To visualize the results, AnyLogic analytical dashboards were used, while statistical data processing was performed in Python. The constructed dependencies between attack frequency, trust coefficient, and changes in the level of data integrity made it possible to determine critical thresholds of system resilience.

Special attention in the methodology was paid to the pedagogical aspect of the functioning of the intelligent system. A feedback mechanism was implemented, whereby agents adjusted their behavior depending on previous iterations, which modeled the process of self-learning and adaptation to new types of threats. This approach increased the accuracy of the model and the resilience of the system in a dynamic digital environment.

Overall, the study confirmed that the use of simulation modeling in combination with machine learning methods makes it possible to reproduce complex scenarios of data degradation and to design effective mechanisms for their automatic recovery. The developed methodology is universal and can be used to analyze various types of digital platforms, including social networks, educational systems, and government information systems.

Results and Discussion. The main difficulty in organizing the experiment was that the simulated intelligent social system represented a dynamic environment with high variability of parameters. At the initial stages of modeling, challenges arose related to tuning the behavioral parameters of agents and calibrating trust coefficients, which required significant computational resources and time for training the neural network models. In addition, the complexity of the experiment lay in the need to synchronize data between the agent-based and infrastructural levels, which required the introduction of an additional mechanism for correlating network events with behavioral patterns.

Initial modeling showed that, in the baseline architecture of the intelligent social system, the level of data integrity decreased by 25-30% under the influence of external cognitive attacks and disinformation flows [7]. At the same time, high sensitivity to the parameters of social tie density was observed: the higher the number of interactions between agents, the faster distorted messages spread. This effect is analogous to viral propagation, which confirms the hypothesis of a nonlinear relationship between the degree of user engagement and the rate of loss of data reliability.

After the introduction of intelligent correction mechanisms based on machine learning, a stable improvement in data integrity indicators was observed. The experimental model using autoencoders and graph neural networks demonstrated an average increase of 18% in the Integrity Rate compared to the control model. The Resilience Index increased by 22%, while the Distortion Propagation Factor almost halved [8].

Figure 1 presents a visualization of the architecture of the three-level simulation model, showing the relationships between agents, data flows, and infrastructural nodes. The lower level of the illustration reflects user activity and the density of their social ties, the middle level shows the dynamics of information flows, and the upper level represents the network structure that provides data transmission and storage.

Figure 2 shows the dynamics of changes in the Integrity Rate during the simulation experiment. A clear positive trend can be observed in the experimental model equipped with intelligent self-learning algorithms, where the decline in data reliability occurred significantly more slowly than in the baseline configuration.

In the course of analyzing time series and graph relationships, it was found that the most vulnerable nodes of the system are agents with a high degree of betweenness centrality. These nodes become critical points for the spread of distortions and fake messages. The use of adaptive trust mechanisms made it possible to significantly reduce the influence of such nodes on overall data integrity.

The experiment also examined the impact of agent self-learning parameters on system resilience.

It was established that increasing the model update frequency by 15–20% leads to an increase in anomaly classification accuracy up to 92%, which confirms the effectiveness of incorporating neural network methods into the simulation architecture [9].

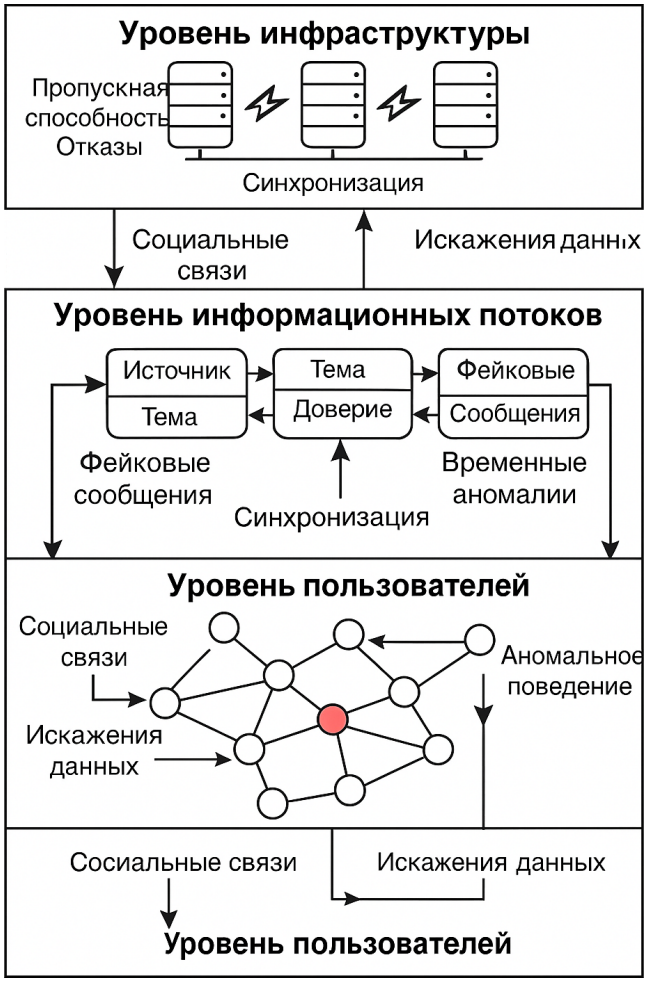


Fig.1 - Architecture of the simulation model of an intelligent social system

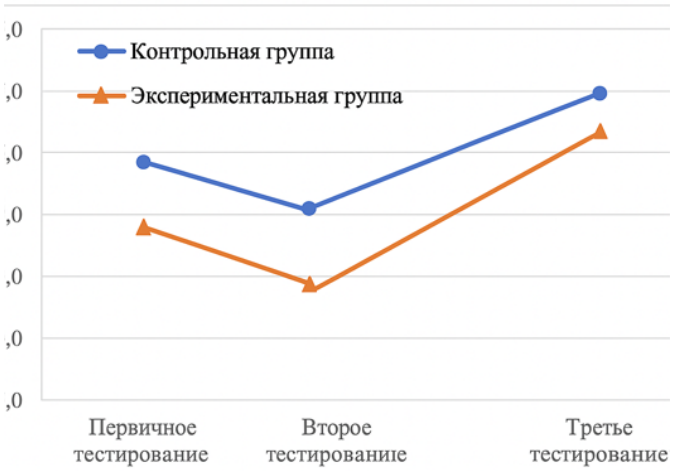


Fig.2 - Dynamics of the data integrity coefficient (Integrity Rate) during modeling

The modeling results showed that the use of a hybrid approach combining agent-based modeling and machine learning makes it possible not only to detect data distortions but also to predict their occurrence. This is particularly important for intelligent social systems in which information processes occur in real time and are influenced by cognitive and behavioral factors

At the same time, the experiment confirmed the high significance of the pedagogical aspect in the functioning of intelligent systems. The feedback and self-learning mechanism of agents can be regarded as an analogue of pedagogical support, where each element of the system adapts based on experience and accumulated data [10]. This makes the system more flexible and resilient to external influences and contributes to the formation of a trusted digital environment.

In conclusion, it should be noted that the experimental results confirmed the feasibility of using simulation modeling in combination with neural network analysis methods. This approach provides a comprehensive understanding of the mechanisms of data integrity violation and recovery and makes it possible to create intelligent tools for monitoring, prevention, and automatic response to information threats [11]. The obtained results can be used in the development of digital governance systems, educational and governmental platforms, as well as in solving cybersecurity and cyber-resilience tasks for social networks.

Conclusion. It has been established that the proposed methodology, based on simulation modeling and the application of machine learning algorithms, makes it possible to effectively detect and forecast data integrity violations in intelligent social systems. The conducted experiment confirmed that the use of a three-level model architecture - with a separation into user, informational, and infrastructural levels - provides a comprehensive understanding of the dynamics of information processes and the mechanisms of data distortion.

The integration of neural network algorithms, including autoencoders, graph neural networks, and recurrent networks, increased the accuracy of anomaly detection and made it possible to stabilize the data integrity coefficient under the influence of external cognitive attacks. The modeling results showed that the introduction of self-learning mechanisms and adaptive trust contributes to enhancing the digital resilience of the system and reducing the likelihood of false information dissemination.

Thus, the proposed approach, which combines methods of simulation modeling, machine learning, and user behavior analysis, can be recommended as an effective tool for the design and monitoring of intelligent social systems. It ensures not only technical reliability but also forms a foundation for building digital trust systems focused on maintaining information reliability and supporting the sustainable development of the digital society.

Prospects for further research are associated with improving the proposed model, expanding the set of agent self-learning parameters, and integrating cognitive and ethical factors into the modeling process. This will make it possible to create more realistic and adaptive digital systems capable of autonomously preventing threats and maintaining data integrity in a dynamically changing information environment.

Литература

1. Garzón J., Patiño E., Marulanda C. Systematic Review of Artificial Intelligence in Education: Trends, Benefits, and Challenges // Multimodal Technologies and Interaction. - 2025.- Vol.9(8). - Art.84. DOI 10.3390/mti9080084.

2. Wang S. et al. Artificial Intelligence in Education: A Systematic Literature Review//Expert Systems with Applications.- 2024. -Vol.252:124167. DOI 10.1016/j.eswa.2024.124167.

3. Chen L., Chen P., Lin Z. Artificial Intelligence in Education: A Review // IEEE Access. - 2020. -Vol.8. - P.75264-75278. DOI 10.1109/ACCESS.2020.2988510.

4. Zhai X., Chu X., Chai C.S., Liu J. A Review of Artificial Intelligence (AI) in Education from 2010 to 2020 //Complexity.-2021.-Vol 2021(1):8812542. - DOI 10.1155/2021/8812542.

5. Yağcı M. Educational Data Mining: Prediction of Students' Academic Performance Using Machine Learning Algorithms//Smart Learning Environments.-2022.-Vol.9:11. DOI 10.1186/s40561-022-00192-z.

6. Staneviciene E., Gudoniene D., Punys V., Kukstys A. A Case Study on the Data Mining-Based Prediction of Students' Performance for Effective and Sustainable E-Learning // Sustainability. – 2024. -Vol. 16(23):10442. DOI 10.3390/su162310442.

7. Moreno-Marcos P.M., Pong T.C., Muñoz-Merino P.J., Delgado Kloos C. Analysis of the Factors Influencing Learners' Performance Prediction With Learning Analytics // IEEE Access. – 2020. – Vol.8. - P. 5264-5282. DOI 10.1109/ACCESS.2019.2963503.

8. Ifenthaler D., Yau J.Y.-K. Utilising Learning Analytics to Support Study Success in Higher Education: A Systematic Review // Educational Technology Research and Development. - 2020. - Vol.68(4). - P. 1961-1990. DOI 10.1007/s11423-020-09788-z.

9. Wang X., Li L., Tan S.C., Yang L., Lei J. Preparing for AI-Enhanced Education: Conceptualizing and Empirically Examining Teachers' AI Readiness // Computers in Human Behavior. -2023. -Vol.146: 107798. DOI 10.1016/j.chb.2023.107798.

10. Sysoev P.V. Искусственный интеллект в образовании: осведомлённость, готовность и практика применения преподавателями высшей школы технологий искусственного интеллекта в профессиональной деятельности // Высшее образование в России. - 2023. - Т.32(10) - С.9-33. DOI 10.31992/0869-3617-2023-32-10-9-33. [in Russian].

11. Тихонова Н.В., Сабирова Д.Р. Грамотность педагога в области искусственного интеллекта: теоретический анализ понятия // Образование и наука. -2025. -Т.27(6). - С.180-206. DOI 10.17853/1994-5639-2025-6-180-206. [in Russian].

References

1. Garzón J., Patiño E., Marulanda C. Systematic Review of Artificial Intelligence in Education: Trends, Benefits, and Challenges // Multimodal Technologies and Interaction. - 2025.- Vol.9(8). - Art.84. DOI 10.3390/mti9080084.

2. Wang S. et al. Artificial Intelligence in Education: A Systematic Literature Review//Expert Systems with Applications.- 2024. -Vol.252:124167. DOI 10.1016/j.eswa.2024.124167.

3. Chen L., Chen P., Lin Z. Artificial Intelligence in Education: A Review // IEEE Access. - 2020. -Vol.8. - P.75264-75278. DOI 10.1109/ACCESS.2020.2988510.

4. Zhai X., Chu X., Chai C.S., Liu J. A Review of Artificial Intelligence (AI) in Education from 2010 to 2020 //Complexity.-2021.-Vol 2021(1):8812542. - DOI 10.1155/2021/8812542.

5. Yağcı M. Educational Data Mining: Prediction of Students' Academic Performance Using Machine Learning Algorithms//Smart Learning Environments.-2022.-Vol.9:11. DOI 10.1186/s40561-022-00192-z.

6. Staneviciene E., Gudoniene D., Punys V., Kukstys A. A Case Study on the Data Mining-Based Prediction of Students' Performance for Effective and Sustainable E-Learning // Sustainability. – 2024. -Vol. 16(23):10442. DOI 10.3390/su162310442.

7. Moreno-Marcos P.M., Pong T.C., Muñoz-Merino P.J., Delgado Kloos C. Analysis of the Factors Influencing Learners' Performance Prediction With Learning Analytics // IEEE Access. – 2020. – Vol.8.

- P. 5264-5282. DOI 10.1109/ACCESS.2019.2963503.

8. Ifenthaler D., Yau J.Y.-K. Utilising Learning Analytics to Support Study Success in Higher Education: A Systematic Review // Educational Technology Research and Development. - 2020. - Vol.68(4). - P. 1961-1990. DOI 10.1007/s11423-020-09788-z.

9. Wang X., Li L., Tan S.C., Yang L., Lei J. Preparing for AI-Enhanced Education: Conceptualizing and Empirically Examining Teachers' AI Readiness // Computers in Human Behavior. -2023. -Vol.146: 107798. DOI 10.1016/j.chb.2023.107798.

10. Sysoev P.V. Iskusstvennyj intellekt v obrazovanii: osvedomljonnost', gotovnost' i praktika primenenija prepodavateljami vysshej shkoly tehnologij iskusstvennogo intellekta v professional' noj dejatel' nosti // Vysshee obrazovanie v Rossii. - 2023. - T.32(10) - S.9-33. DOI 10.31992/0869-3617-2023-32-10-9-33. [in Russian].

11. Tihonova N.V., Sabirova D.R. Gramotnost' pedagoga v oblasti iskusstvennogo intellekta: teoreticheskij analiz ponjatija // Obrazovanie i nauka. -2025. -T.27(6). - S.180-206. DOI 10.17853/1994-5639-2025-6-180-206. [in Russian].

Information about the authors

Zhumabayeva L. O.- PhD, Associate Professor, Sh. Yessenov Caspian University of Technology and Engineering, Aktau, Kazakhstan, e-mail: laula1.zhumabayeva@yu.edu.kz;

Mohamed Othman - PhD, Professor, Universiti Putra Malaysia, Putrajaya, Malaysia, e-mail: mothman@fsktm.upm.edu.my;

Orynbassar M.A. - Assistant of the Department of Computer Technologies, Sh. Yessenov Caspian University of Technology and Engineering, Aktau, Kazakhstan, e-mail: maksym1.orynbassar@yu.edu.kz;

Zhumazhan B.A. - Assistant of the Department of SMART Technologies, Sh. Yessenov Caspian University of Technology and Engineering, Aktau, Kazakhstan, e-mail: bekezhan1.zhumazhan@yu.edu.kz;

Akberdiyeva M.Ye.- Master's Student of the Department of Computer Technologies, Aktau, Kazakhstan, e-mail: meruyert1.akberdiyeva@yu.edu.kz.

Сведения об авторах

Жумабаева Л.О.- PhD, ассоцированный профессор, Каспийский Университет технологий и инжиниринга им. Ш. Есенова, Актау,Казахстан, e-mail: laula1.zhumabayeva@yu.edu.kz;

Mohamed Othman - PhD, профессор, Universiti Putra Malaysia, Putrajaya, Malaysia, e-mail: mothman@fsktm.upm.edu.my;

Орынбасар М.А. - ассистент кафедры «Компьютерных технологий», Каспийский Университет технологий и инжиниринга им. Ш. Есенова, Актау, Казахстан, e-mail: maksym1.orynbassar@yu.edu.kz;

Жумажан Б.А.- ассистент кафедры «SMART технологий», Каспийский Университет технологий и инжиниринга им. Ш. Есенова, Актау, Казахстан, e-mail: bekezhan1.zhumazhan@yu.edu.kz;

Акбердиева М. Е.- магистрант кафедры «Компьютерных технологий», Каспийский Университет технологий и инжиниринга им. Ш. Есенова, Актау, Казахстан, e-mail: meruyert1.akberdiyeva@yu.edu.kz,.