I.J. Modern Education and Computer Science, **2024, 5, 21-32**
Published Online on October 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2024.05.02

The Effect of Threats from Using the Artificial Intelligence on the Educational Process in the Context of Information Security: A Methodological Approach to Modeling and Ordering Impact Levels

Myroslav Kryshtanovych*
Department of Pedagogy and Innovative Education, Lviv Polytechnic National University, Lviv, 79000, Ukraine
Email: myroslav.f.kryshtanovych@lpnu.ua
ORCID iD: https://orcid.org/0000-0003-1750-6385
*Corresponding Author

Iryna Gavrysh
Department of Primary and Professional Education, H.S. Skovoroda Kharkiv National Pedagogical University, Kharkiv, 61002, Ukraine
Email: Irina.gavrysh@gmail.com
ORCID iD: https://orcid.org/0000-0002-0173-1855

Oleksandra Khltobina
Department of Theory and Technology of Pre-school Education and Art Disciplines, H.S. Skovoroda Kharkiv National Pedagogical University, Kharkiv, 61002, Ukraine
Email: xoltobina@ukr.net
ORCID iD: https://orcid.org/0000-0002-2155-7129

Ihor Havrylov
Department of Professional Education, Grigory Skovoroda University in Pereyaslav, Pereyaslav, 71002, Ukraine
Email: 19701990Igor@gmail.com
ORCID iD: https://orcid.org/0000-0003-0436-3776

Yevhen Gren
Department of Professional Education, Grigory Skovoroda University in Pereyaslav, Pereyaslav, 71002, Ukraine
Email: yevhengren@gmail.com
ORCID iD: https://orcid.org/0009-0004-0275-038X

Received: 06 April, 2024; Revised: 29 May, 2024; Accepted: 15 August, 2024; Published: 08 October, 2024

Abstract: The main purpose of the article is to highlight and determine the level of influence of the most significant threats from the use of artificial intelligence in the educational process in the context of ensuring information security. To achieve this goal, the research methodology involves the use of an expert analysis method, which, through the Delphi method, will help to identify the most significant threats to the use of artificial intelligence in the educational process, a paired comparison method, which is necessary to implement the hierarchical analysis method, which in turn aims to organize a certain list of experts. As a result of the study, the most significant modern threats to the use of artificial intelligence in the educational process in the context of ensuring information security were identified. The resulting matrix of hierarchical ordering of threats made it possible to divide them into those that require immediate intervention and those that are less important. The innovativeness of the results obtained is revealed through the established methodological approach to modeling the ordering of the influence of threats from the use of artificial intelligence on the educational process in the context of ensuring information security. The study is limited by taking into account only the specifics of the educational process in Ukraine.

Index Terms: Artificial Intelligence, Education, Information Security, threats

1. Introduction

1.1 Highlighting the relevance of the selected problem

Today there is an active integration of artificial intelligence technologies into all spheres of public life. The field of higher education is no exception. Thus, education adapted to the needs of our time, one of which is the active use of digital technologies, can be considered effective and meets the needs of the labor market. The use of artificial intelligence technologies in the education system can significantly improve the educational process, bringing new opportunities and educational tools to it. The introduction of artificial intelligence technologies also makes it possible to adapt the educational process to the individual characteristics of each student, through the formation of individualized plans, assessment systems and other means. Such individualized plans allow you to adapt the educational process to the strengths and weaknesses of each student, thereby making learning easier and more effective. This feature of the use of artificial intelligence is the main distinguishing feature of the latter from traditional methods of education, the use of which is aimed at creating and ensuring a single unified educational process that does not take into account the individual needs of students, but is only aimed at achieving weighted average results.

At the same time, in addition to directly influencing the educational process, artificial intelligence technologies can be used in the higher education administration system in matters of drawing up plans, monitoring knowledge, generating ratings and other processes in which large amounts of data need to be analyzed. In general, the use of artificial intelligence technologies can significantly facilitate the work process for all participants in the educational process and the functioning of the educational institution.

At the same time, the wide possibilities of using artificial intelligence can lead to serious problems and threats in the field of information security. Thus, significant amounts of personal data provided to artificial intelligence for processing can lead to violations of confidentiality and unlawful actions with personal information. Given this, the use of artificial intelligence technologies in the educational process of higher education offers significant benefits for all participants in this process. But at the same time, irresponsible and uncontrolled use of these technologies can lead to information security threats. This fact requires higher education institutions to use cybersecurity measures to identify and assess these threats. This situation highlights the importance of finding a balanced approach that takes advantage of artificial intelligence while maintaining the security of the information environment of the educational process.

The integration of artificial intelligence technologies in education has considerable potential to revolutionize learning experiences through personalized teaching methods and streamlined administrative tasks. However, it also introduces significant risks, particularly in terms of reinforcing existing societal biases. These technologies are often developed using large datasets that reflect historical biases. When applied to educational processes such as grading, admissions, or content creation, there's a risk that these biases could influence decisions, disproportionately affecting minority or disadvantaged groups. Additionally, the implementation of sophisticated algorithms in educational settings raises serious concerns about data privacy and security. Schools collect sensitive information about students, including academic performance, personal backgrounds, and behavioral patterns.

The introduction of artificial intelligence into higher education introduces a number of ethical considerations. The biases inherent in artificial intelligence algorithms, if not carefully managed, could inadvertently perpetuate discrimination or inequality. Ensuring that artificial intelligence systems are designed and implemented in a fair and unbiased manner is crucial to their successful integration into the educational process. It's been said that while the use of artificial intelligence in higher education presents clear benefits in terms of personalization, efficiency, and engagement, it also requires careful management of information security, ethical, and interpersonal concerns. Balancing these aspects is essential to harnessing the full potential of artificial intelligence in enriching the educational experience without compromising on privacy, equity, or the human touch that lies at the heart of learning.

1.2 Structure, purpose and key objects of research

The structure of the article provides a review of the literature on the topic of the article, a presentation of the key methods used in the study, highlighting the key results of the study and their discussion. The main purpose of the article is to highlight and determine the level of influence of the most significant threats from the use of artificial intelligence in the educational process in the context of ensuring information security. The object of the study is the educational process and the information security system.

2. Literature Review

2.1 The role of artificial intelligence in higher education

Before implementing the planned research methods, it is also important to analyze the relevant literature and studies related to the topic. This is especially important for the further correct identification of threats that may arise during the use of artificial intelligence in the educational process.

For example, scientists Kolidakis et al. [1] were among the first to scientifically substantiate the advantages of using artificial intelligence in the educational process. The authors were able to demonstrate these benefits through artificial intelligence modeling of schedules, training programs, and rating schemes. This work was one of the first to declare the possible advantages of using artificial intelligence to analyze large databases in the education system. Extending the results described above is the work of Iskajyan et al. [2], exploring the general advantages of using modern digital technologies in various areas of society, including the sphere of higher education. So, the authors formulate the statement that any sphere of modern society is one way or another integrated into the information society, and given this, the effective functioning of all modern spheres of society is impossible without the active use of digital technologies. At the same time, the authors determine not only the advantages of using digital technologies, but also possible problems and dangers.

At the same time, Alazam et al. [3] explores possible ways to optimize the process of integrating digital technologies into various spheres of society using the example of e-commerce platforms. Their research is of interest from a scientific point of view in that the authors demonstrate the importance of taking into account clear legal, economic and ethical frameworks in the use of artificial intelligence technologies and formulate principles for the safe use of modern digital technologies, including the principles of confidentiality, which is no less important for education. . Luo's study [4] also addresses the security issues of using digital technologies, in particular artificial intelligence technologies. Their research suggests the use of models for compliance with data security protocols, which is especially relevant in the field of implementation of the educational process, where there is a real need to protect confidential and personal information of students and teachers. Also interesting is the study by Sylkin et al. [5], aimed at developing risk management models in the system of various types of security. Such research is especially important in the context of identifying and forming an effective system to counter threats that may arise when integrating artificial intelligence technologies into the educational process.In sum, the literature presents a complex picture of the role of artificial intelligence in higher education. While the potential for enhanced efficiency, personalized learning, and administrative effectiveness is clear, so too are the challenges related to information security, data privacy, and ethical considerations. As such, any methodological approach to modeling and ordering the impact levels of threats from artificial intelligence must carefully balance these factors, drawing on the insights provided by existing research to navigate the nuanced landscape of artificial intelligence in education.

2.2 The multifaceted implications of artificial intelligence in higher education, particularly in the realm of information security

In a study by Raso et al. [6] provides an in-depth and detailed analysis of the implications of the use of artificial intelligence in the context of respect for key human rights. Thus, the study allows us to understand the ethical contradictions of using artificial intelligence technologies in education. Their research raises the question that the uncontrolled use of artificial intelligence technologies in education may affect the equity and fairness of the provision and quality of educational services. At the same time, Al Azzam's [7] in his work explores modern activity and areas of work of cybercrime. The authors determine that today manifestations of cybercrime can be traced in all spheres of society, including in the field of education, and the formation of appropriate measures is an equally important task for both the economic sphere and the educational system.

A targeted analysis of the education sector is carried out by Häkkinen et al. [8], substantiating the importance of developing information and digital competencies in both teachers and students, which are important not only for the ability to operate modern digital technologies, but also for understanding security measures when working with them.

Kryshtanovych et al. offer a model for the digitalization of education management, providing a framework that could guide the strategic implementation of artificial intelligence in higher education institutions, ensuring that digitalization efforts align with sustainable development goals. Bobrova et al. propose an algorithmic framework for information systems that ensure sustainable development and national security, suggesting a methodological approach that could be applied to safeguarding the information security of educational institutions in the digital age [9,10].

Berzosa et al. evaluate sustainability assessment tools for higher education, contributing to the conversation on sustainable practices within higher education that could be enhanced through the strategic use of artificial intelligence. Shkvyr et al. examine the integration of information technology in digital education, offering insights into the mathematical modeling of technology integration that can inform the development of artificial intelligence applications in higher education [11,12]. This comprehensive review of literature illustrates the multifaceted implications of artificial intelligence in higher education, particularly in the realm of information security. The studies reviewed provide a basis for understanding both the potential enhancements artificial intelligence can bring to educational processes and the

critical challenges it presents, especially in terms of data security, ethical considerations, and the need for sustainable, risk-managed integration strategies.

Kryshtanovych et al., as cited in reference [14], discuss a methodological approach to fostering creative thinking among students in creative professions. This perspective is crucial for understanding how artificial intelligence might impact not only the technical aspects of education but also the creative and ethical dimensions. Their insights into methodological rigor and educational outcomes offer valuable parallels to the analysis of AI's influence on educational practices, highlighting the need for methodologies that equally consider ethical and developmental impacts. The ethical concerns surrounding artificial intelligence are critically analyzed by Bietti in reference [15]. Bietti's exploration of the transition from "ethics washing" to "ethics bashing" in the tech industry provides a cautionary tale for artificial intelligence applications in education. This reference is instrumental in framing the discussion about the ethical implications of artificial intelligence deployment in educational settings, where the integrity of educational outcomes and student privacy must be paramount. Kim and Shin, as seen in reference [16], focus on the development of tests for artificial intelligence ethical awareness. Their work underscores the importance of integrating ethical considerations into the development and application of artificial intelligence technologies in education. The creation and implementation of such tests could serve as a benchmark for educational institutions looking to incorporate artificial intelligence, ensuring that these technologies are used responsibly and ethically. Finally, reference [17] examines the stages of digital transformation in educational institutions within the context of regional sustainable development. Their discussion on the systematic approach to digital transformation highlights the complexities and multi-faceted nature of integrating advanced technologies like artificial intelligence into educational environments. Their findings provide a framework for understanding the layered impact of artificial intelligence on information security and educational processes.

2.3 The main gaps in literature

In the context of higher education institutions and their students, the exploration of artificial intelligence's role and its associated risks requires a nuanced understanding, revealing several gaps in current academic literature. These gaps are particularly critical when considering the dual objectives of leveraging artificial intelligence to enhance the educational process and ensuring robust information security measures (Fig.1).

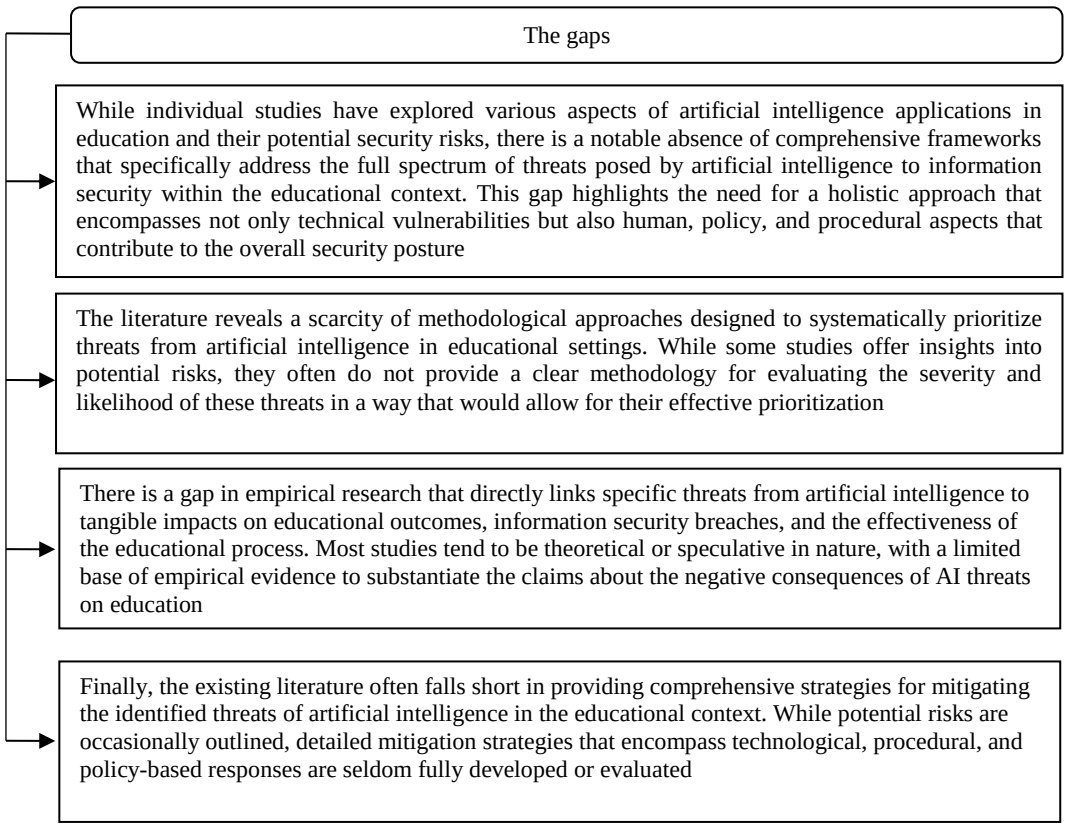

Fig. 1. The main gaps in literature

Considering a number of gaps in the scientific literature, we set our article as a scientific task to propose a new methodological approach to modeling the ordering of the levels of influence of threats from artificial intelligence technologies on the educational process in the context of ensuring information security. Moreover, the region that we have chosen concerns Ukraine and its peculiarities. The reason for this choice is revealed that the team of authors of the article works there.

3. Methodology

3.1 Methods for identifying threats

At the first stage of the selected methodology, the method of expert analysis will be used. In the process of using this method, expert groups of specialists in the field of artificial intelligence, information security, security of the educational process and specialists in the field of education management were formed. The selection of experts was based on the criteria of their professional competence and experience, as well as experience in participation in scientific research. In the process of expert analysis, groups of experts identified a list of key threats that have the most significant impact in the process of using artificial intelligence technologies in the field of education. After conducting direct expert analysis, we used the Delphi method, which made it possible to structure and systematize expert opinions in order to obtain a consensus of expert decisions regarding the level of importance of each threat. Using the Delphi method makes it possible to avoid bias and subjectivity of expert opinions. Ultimately, we received a list of seven key threats that have the greatest impact on the education system in the process of introducing artificial intelligence technologies into it.

These experts contribute deep knowledge of AI technology, its capabilities, limitations, and the specific ways it can be integrated into educational environments. Their expertise is crucial in understanding the technical nuances and potential impacts of AI applications in higher education. Experts in this area look specifically at the security concerns within educational institutions, such as safeguarding student information and ensuring secure teaching methodologies. Their insights help bridge the gap between general security practices and specific educational needs.

3.2 Methods for modeling

After implementing the above steps of the methodology, the paired comparison method will be used next. In the context of our method, this method will be used for pairwise comparison of each threat relative to the other, while determining the level of their importance and influence on the process under study. As a result of implementing the paired comparison method, we will receive a ranked list of threats affecting the education system in the process of integrating artificial intelligence technologies into it. Based on the results of the paired comparison method, in addition to it, we will use the hierarchical analysis method to further clarify the level of importance of a particular threat. This method involves forming a structure of identified threats in a hierarchy from the most significant to the least significant. Thus, the synthesis of these two methods makes it possible to clearly understand the level of importance of each threat of artificial intelligence to the educational process and, based on this, to formulate effective strategies for managing this process.

The methodology employed in this study is designed to meticulously evaluate the impact of threats from the use of artificial intelligence in the educational process of higher education institutions, with a particular focus on information security. The essence of our methodological approach is rooted in a combination of expert analysis, the Delphi method, and a paired comparison method within a hierarchical analysis framework. This multi-faceted methodology aims not only to identify and prioritize the most significant threats but also to model their levels of influence on the educational process in the context of information security.

4. Results

4.1 Characteristics of threats

Based on the results of the expert analysis method, we have identified key threats that impact the education system and the educational process when integrating artificial intelligence technologies into it, and pose a danger to information security:

T1 Operational origins are given. One of the key threats in the process under study is the high risk of data leakage from educational systems that integrate artificial intelligence technologies. Such a vulnerability not only poses a threat to confidential data and personal information of teaching and student staff in higher education, but may pose risks for other criminal activities - disinformation, data fraud and data falsification. Such a threat can become a destructive factor not only for the confidential data of teachers and students, but also for the reputation of a higher education institution.

T2. Manipulation of Educational Content. Influenced by the propagation of misinformation, this threat involves the intentional distortion or manipulation of educational materials. The integrity of academic content is crucial for maintaining educational standards and ensuring that students receive accurate, unbiased information.

T3. Bias in Educational Algorithms. The quality and fairness of automated educational tools and resources can be compromised by underlying biases in their design. This can lead to unequal educational opportunities, reinforcing existing social inequalities. The propagation of misinformation can exacerbate this by skewing the data sets used for training such systems, further entrenching biased outcomes.

T4. Unauthorized Access to Sensitive Information. Stemming from exploitable data breaches, this threat involves unauthorized individuals gaining access to sensitive educational resources, personal student data, or proprietary research. This can lead to academic fraud, identity theft, and a breach of privacy.

T5. Propagation of Misinformation. A critical threat in its own right, the spread of false or misleading information can undermine the quality of education, influence the development and implementation of biased educational algorithms, and contribute to the manipulation of educational content. This is particularly concerning in an era where digital learning materials and online resources are increasingly prevalent.

T6. Compromise of Academic Integrity. Independent of the direct influence of other threats, this concern revolves around the use of technology to facilitate academic dishonesty, including plagiarism and the unauthorized sharing of copyrighted materials. This undermines the value of academic credentials and the integrity of the educational process.

T7. Undermining of Institutional Trust and Credibility. The culmination of threats from exploitable data breaches, particularly through the undermining of access control and the spread of misinformation, can significantly erode trust in educational institutions. This not only affects student and faculty confidence in the security and fairness of the educational process but also impacts the credibility of academic research and credentials in the broader societal context.

4.2 Modeling results

As we can see, each of the threats is assigned a mathematical designation in the form T. In general, there is a set: T = {T1, T2, T3, T4, T5, T6, T7}. Thus, this set allows us to construct a matrix of size 7 by 7, respectively. The matrix is filled in so that the following equality (1) is determined through experts:

$$T_{ij}=\begin{cases}1, if\ one\ threat\ affects\ another\\ 0\ if\ not\end{cases} \quad (1)$$

Thus, we build a dependence matrix based on the results of a pairwise comparison of certain threats from the use of artificial intelligence in the educational process today that pose a danger to information security (2):

	$T1$	$T2$	$T3$	$T4$	$T5$	$T6$	$T7$
$T1$	0	0	1	1	1	0	1
$T2$	0	0	0	0	0	0	0
$T3$	0	0	0	0	0	0	0
$T4$	0	0	0	0	0	0	0
$T5$	0	1	1	1	0	0	0
$T6$	1	0	1	1	1	0	0
$T7$	0	0	0	0	1	0	0

(2)

Next, using the main matrices (2), it is possible to build a graph using graph theory that will show the connections between certain dangers of introducing artificial intelligence in educational activities for higher education in Ukraine (Fig. 2).

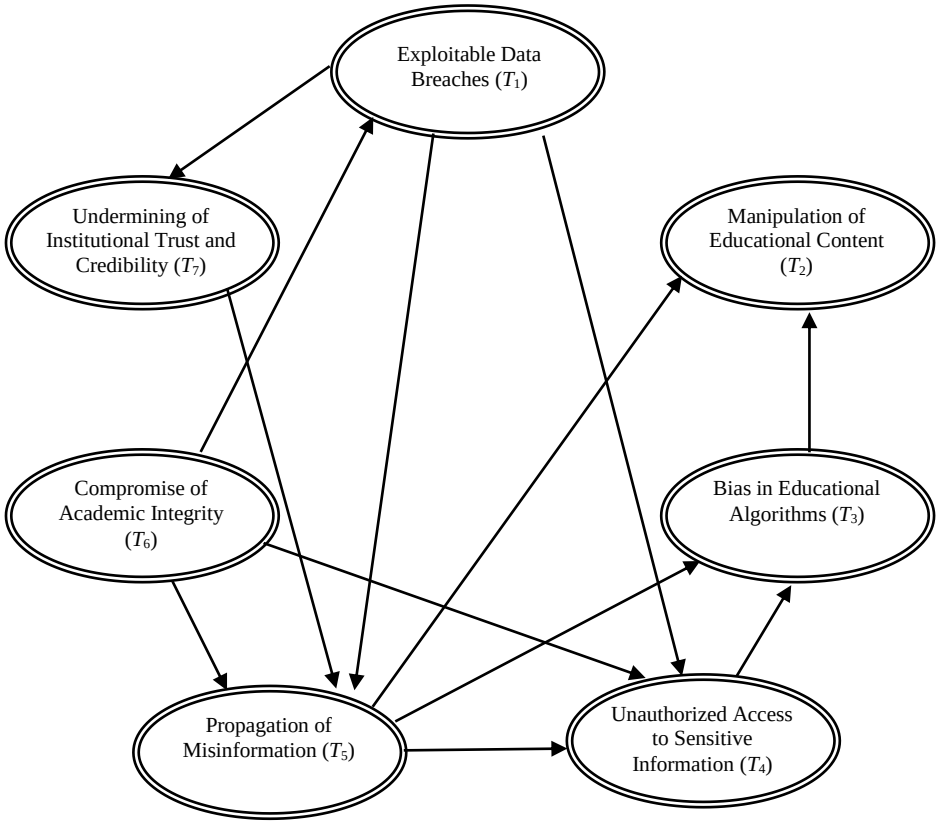

Fig. 2. Graph of connections between certain threats from the use of artificial intelligence in the educational process for higher education institutions in Ukraine

At the same time, we further note that it is necessary to build a reachability matrix in which the following equality must also be fulfilled through expert analysis (3):

$$T_{ij}=\begin{cases}1, if\ the\ threat\ depends\ on\ another\\ 0\ if\ not\end{cases} \quad (3)$$

Based on this, we will build a matrix of the reach of threats caused by the use of artificial intelligence in the educational process on the territory of Ukraine (4):

$$\begin{array}{c|ccccccc} & T1 & T2 & T3 & T4 & T5 & T6 & T7 \\ T1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ T2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ T3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ T4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ T5 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ T6 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ T7 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \quad (4)$$

At the same time, we note that from one threat there is a path to another, we denote it as D(Ti). Moreover, if the connection is connected, this means that the threat affects the threat in a certain way. Let us denote the set of predecessor vertices of the graph as P(Ti). In this case, the section D and P will give us a new set (5):

$$N(T_i) = D(T_i) \cap P(T_i) \quad (5)$$

At the same time, if the condition N(Ti) = P(Ti) is fulfilled, it means that the threat will constitute the first level of impact severity. This continues until all are removed and only one, the most important, remains (Table 1).

Table 1. Iterative table of formation of levels of influence of threats of application of artificial intelligence in educational processes

Ti	$D(T_i)$	P(Ti)	N(Ti)
1	|1| |2| |3| |4| |5| |7|	|1| |6|	1
2	|2|	|1| |2| |3| |4| |5| |6| |7|	2
3	|2| |3|	|1| |3| |4| |5| |6| |7|	3
4	|2| |3| |4|	|1| |4| |5| |6| |7|	4
5	|2| |3| |4| |5|	|1| |5| |6| |7|	5
6	|1| |2| |3| |4| |5| |6| |7|	|6|	6
7	|7|	|1| |6| |7|	7

As we can see from Table 1, the equality is fulfilled exactly for the 6th threat. It will be the lowest level in the influence hierarchy. Next, "6" is removed from the table and so on until only one remains. We bypass those intermediate calculations and extractions and immediately present the matrix of the hierarchy of threats of the use of artificial intelligence in the educational process of Ukraine (Table 2).

Table 2. The matrix of the hierarchy of threats of the use of artificial intelligence in the educational process of Ukraine

Level 7 (The most important)	T2	Manipulation of Educational Content
Level 6	T3	Bias in Educational Algorithms
Level 5	T4	Unauthorized Access to Sensitive Information
Level 4	T5	Propagation of Misinformation
Level 3	T7	Undermining of Institutional Trust and Credibility
Level 2	T1	Exploitable Data Breaches
Level 1 (The least weighty)	T6	Compromise of Academic Integrity

In order to counteract the facts of manipulation of educational content, it is important to implement an integrated approach, including measures to ensure the accuracy and integrity of information. Thus, higher education institutions should form management strategies that would combine strict and step-by-step systems for monitoring educational content. These systems should include expert reviews, cooperation with international educational platforms and other initiatives, the implementation of which would make it possible to quickly verify the accuracy and reliability of educational materials. At the same time, it is important to formulate and strictly adhere to the ethical principles of the formation of educational content. Thus, involving the academic community, conducting seminars and group

assessments on the quality and morality of educational resources will be a powerful factor in creating an ethical framework for the use of artificial intelligence in the educational process. We must also not forget about the importance of international communication in the matter of establishing and improving standards for the implementation of digital education and information security. The experience of other countries or individual higher education institutions can be helpful in this complex and complex issue. As we can see, solving this problem requires the implementation of an integrated and multi-vector approach to ensure a high level of information security and safe use of artificial intelligence capabilities in higher education institutions.

5. Discussions

5.1 Comparison of the obtained results with others

The originality of this research lies in its methodological approach to systematically categorizing the influence of threats posed by the use of artificial intelligence in educational settings, particularly with respect to information security. By employing a combination of expert analysis through the Delphi method and the paired comparison method for hierarchical analysis, the study innovatively creates a structured matrix that not only identifies significant threats but also prioritizes them according to their urgency.

The study by Kopytko and Sylkin [18] presents a detailed analysis of the processes of modeling information support for processes of combating cybercrime. Similar to our study, the emphasis is on the importance of choosing the right comprehensive and structured approach to ensuring information security. At the same time, our study examines the processes under study somewhat more broadly due to the use of a comprehensive research methodology. In addition, our work is more specific, since it examines threats directly related to the educational system and the introduction of artificial intelligence technologies into it. At the same time, Kwon [19] in his work examined the features of the use of artificial intelligence from the point of view of moral consciousness. And although Kwon's findings provide a valuable theoretical basis and include various areas of the educational process, the author did not present clear methods for solving the problem posed and did not provide tools through which the solution of these moral and ethical problems can be integrated into general strategies for managing the educational process or higher institution. education. In contrast to this study, our study offers a specific methodological approach that may be useful in practice.

An interesting study by Kronivets et al. [20], who studied the modern legal framework of artificial intelligence in educational processes. Their analysis provides useful considerations regarding vectors for improving regulatory support in this area. However, despite the detailed analysis and considerations, the authors did not provide specific methods for improving regulatory support. While our research includes not only detailed analysis, but also practical recommendations. The work of Sylkin et al. [21] uses a method of hierarchical ordering of threats to economic security. This study provides key information about the features of ranking threats using the hierarchical ordering method. We have expanded the use of this method through the use of additional research methods to better determine the level of influence of various threats.

Huang and Hsin [22] focused on environmental literacy and sustainable development in schools. While their study is tangentially related in terms of broader educational impacts, our research narrows the focus to artificial intelligence threats within higher education, underscoring the need for specialized security measures in this rapidly evolving field. Kryshtanovych et al. [23] examined information support of public administration during the COVID-19 pandemic. Their focus on information support systems during crises complements our study's emphasis on information security threats from artificial intelligence, highlighting the importance of robust information management in both public administration and higher education.

Saleh et al. [24] and Lim [25] provide insights into the legal management of cryptocurrency assets and moral education in the age of artificial intelligence, respectively. Both studies contribute to the broader discourse on the implications of artificial intelligence and technology in society. Our research adds a specific focus on the security aspect within the educational process, enriching the dialogue with practical, methodological insights. Bilyk et al. [26] investigated modeling ways to increase creativity among psychology students. While focusing on enhancing student creativity, our study provides a framework for understanding and mitigating threats, demonstrating the diverse applications of methodological modeling in education.

5.2 Highlighting the innovativeness of own results

Our study contributes to the existing literature by offering a unique, methodological approach to assessing and prioritizing threats from the use of artificial intelligence in higher education. It highlights the importance of a structured, analytical framework to address information security challenges effectively (Fig.4).

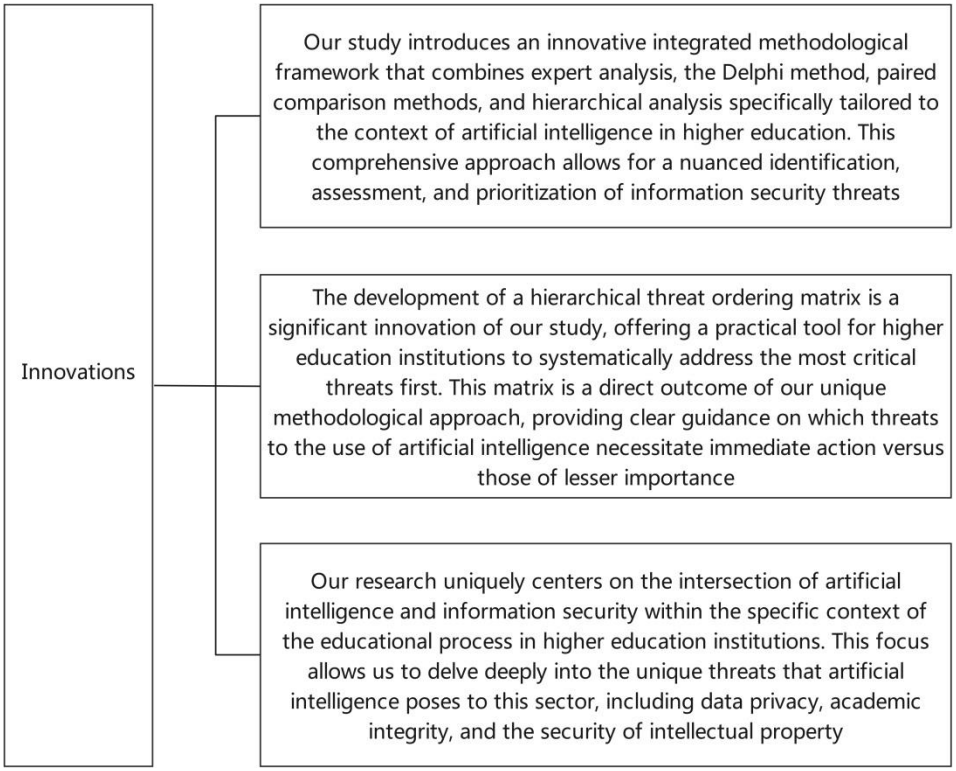

Fig. 4. The main gaps in literature

These innovations not only contribute to the academic discourse on artificial intelligence in education but also offer practical, actionable insights for higher education institutions seeking to navigate the complex landscape of artificial intelligence adoption and information security. Future research building on these innovations could further refine the threat assessment and prioritization process, explore the applicability of the hierarchical threat ordering matrix in other contexts, and continue to address emerging information security threats as artificial intelligence technologies evolve. One of the central achievements of our study was the creation of a matrix that categorizes the identified threats based on their severity and urgency. This hierarchical structure is crucial for prioritizing responses to these threats. By classifying them into categories requiring immediate intervention and those of lesser importance, educational institutions can more effectively allocate resources and implement targeted security measures.

6. Conclusion

6.1 Practical Implications

The complexity and multi-vector nature of the study makes it possible to analyze all possible nuances and aspects of threats that may be caused by the integration of artificial intelligence technologies in the educational process of higher educational institutions. Through an optimized and correct selection of research methods (consisting of expert analysis methods, the Delphi method, the method of paired comparisons and hierarchical analysis), we have identified and ranked a list of key threats that can be caused by the integration of artificial intelligence technologies in the educational process of higher educational institutions. Thus, in the end, a matrix was formed in which threats were classified according to their level of urgency and significance. This ranking allows you to understand the level of influence of each threat and formulate a correct and effective strategy for response and counteraction.

The results of the study have a number of positive practical implications related to institutions of higher education. Thus, the hierarchical ordering matrix can become a key resource for specialists in the security of the information space of the educational process, technologists and politicians involved in the activities and development of the field of higher education. The use of this matrix also allows for a more rational use of available resources when forming targeted strategies to minimize the risks and challenges that arise when using artificial intelligence in the educational process. This is especially true when planning and developing safe educational programs for students of higher education institutions that contain artificial intelligence technologies. In addition, this developed methodological approach is not limited to use only in the field of higher education. The flexibility of the methods used allows to adapt the existing matrix and apply it in other areas where artificial intelligence technologies are currently actively used.

6.2 Limits and Future Research

Despite its contributions, this study is not without its limitations. The scope of the research was specifically tailored to the context of higher education institutions in Ukraine, which may not fully encapsulate the global diversity of threats or the unique challenges faced by institutions in different geographical and regulatory environments. Therefore, the findings may have limited applicability beyond this specific context. Looking forward, there is a clear need for more extensive research that broadens the geographical scope of the study to include a wider array of higher education institutions across different countries and regulatory landscapes. Such research would enhance the generalizability of the findings and provide a more global perspective on the threats posed by artificial intelligence to information security in the educational process. Additionally, future studies should also consider the rapid evolution of artificial intelligence technologies and the emergence of new threats. Continuous monitoring and reassessment of the threat landscape are essential to keep pace with these advancements. There is also a pressing need to explore and develop more sophisticated mitigation strategies and protective measures that can evolve in tandem with the threats they aim to counteract. The development of a hierarchical ordering of threats is particularly innovative. This model categorizes threats into levels based on their need for immediate intervention. Such stratification is crucial for developing tiered security measures and efficiently allocating resources towards the most pressing issues first.

In conclusion, it should be noted that the use of artificial intelligence in the educational process opens up significant opportunities and vectors of development, but at the same time causes the emergence of threats and challenges to information security. Our research is aimed specifically at analyzing this issue and offers a methodological approach to identifying key threats and eliminating them. Thus, the use of our methodology will allow higher education institutions to form a powerful system for protecting their own educational processes from threats caused by the use of artificial intelligence, while ensuring the uninterrupted development of innovations in the educational process.

References

[1] Kolidakis, S.Z., Kotoula, K.M.A., Botzoris, G.N. (2022). School mode choice classification model exploitation though artificial intelligence classification application. Mathematical Modelling of Engineering Problems, Vol. 9, No. 6, pp. 1441-1450. https://doi.org/10.18280/mmep.090601

[2] Iskajyan, S.O., Kiseleva, I.A., Tramova, A.M., Timofeev, A.G., Mambetova, F.A., Mustaev, M.M. (2022). Importance of the information environment factor in assessing a country's economic security in the digital economy. International Journal of Safety and Security Engineering, Vol. 12, No. 6, pp. 691-697. https://doi.org/10.18280/ijsse.120604

[3] Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., Sylkin, O. (2023). Developing an information model for E-Commerce pltforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. Ingénierie des Systèmes d'Information, Vol. 28, No. 4, pp. 969-974. https://doi.org/10.18280/isi.280417

[4] Luo, H.N. (2020). An emergency management system for government data security based on artificial intelligence. Ingénierie des Systèmes d'Information, Vol. 25, No. 2, pp. 207-213. https://doi.org/10.18280/isi.250208

[5] Sylkin, O., Shtangret, A., Ogirko, O., & Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of the application of anti-crisis management: Practical aspect. Business and Economic Horizons (BEH), 14(4), 926–940. https://doi.org/10.15208/beh.2018.63

[6] Raso, F.A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., Kim, L. (2018). Artificial intelligence & human rights: opportunities & risks. Berkman Klein Center Research Publication, (6). https://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439

[7] Al Azzam, F.A.F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. JANUS. NET E-Journal of International Relations, 10(1): 64-81. https://doi.org/10.26619/1647-7251.10.1.5

[8] Häkkinen, P., Järvelä, S., Mäkitalo-Siegl, K., Ahonen, A., Näykki, P., Valtonen, T. (2015). Preparing teacher students for 21st century learning practices (PREP 21): A framework for enhancing collaborative problem solving and strategic learning skills. Teachers and Teaching Theory and Practice, 23(1): 1-17. https://doi.org/10.1080/13540602.2016.1203772

[9] Kryshtanovych, S., Inozemtseva, O., Voloshyna, O., Ostapiovska, I., Dubrova, O. (2023). Modeling the effective digitalization of the education management system in the context of sustainable development. International Journal of Sustainable Development and Planning, Vol. 18, No. 5, pp. 1507-1514. https://doi.org/10.18280/ijsdp.180521

[10] Bobrova, Y., Bobrov, Y., Vavreniuk, S., Bondarenko, O. (2024). Algorithmic framework for an information system ensuring sustainable development and national security. Ingénierie des Systèmes d'Information, Vol. 29, No. 1, pp. 153-159. https://doi.org/10.18280/isi.290117

[11] Berzosa, A., Bernaldo, M.O., Fernández-Sanchez, G. (2017). Sustainability assessment tools for higher education: An empirical comparative analysis. Journal of Cleaner Production, 161: 812-820. https://doi.org/10.1016/j.jclepro.2017.05.194

[12] Shkvyr, O., Dudchak, H., Kazakova, N., Polianovska, O., Sivak, N. (2023). Mathematical modeling of information technology integration in digital education: A regional perspective. Ingénierie des Systèmes d'Information, Vol. 28, No. 3, pp. 603-610. https://doi.org/10.18280/isi.280308

[13] Alazzam, F. A. F., Tubishat, B. M. A.-R., Savchenko, O., Pitel, N., & Diuk, O. (2023). Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. Business: Theory and Practice, 24(2), 594–603. https://doi.org/10.3846/btp.2023.19781

[14] Kryshtanovych, M., Kryshtanovych, S., Stepanenko, L., Brodiuk, Y., & Fast, A. (2021). Methodological approach to determining the main factors for the development of creative thinking in students of creative professions. Creativity Studies, 14(2), 391-404. https://doi.org/10.3846/cs.2021.14806

[15] Bietti, E. (2020). From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy. In Proceedings of the 2020 conference on fairness, accountability, and transparency, TUP, pp. 210-219. https://doi.org/10.1145/3351095.3372860
[16] Kim, G.S., Shin, Y.J. (2021). Study on the development of a test for artificial intelligence ethical awareness. Journal of The Korean Association of Artificial Intelligence Education, 2(1): 1-19. https://doi.org/10.52618/AIED.2021.2.1.1
[17] Kryshtanovych, S., Liakhovych, G., Dubrova, O., Kazarian, H., Zhekalo, G. (2023). Stages of digital transformation of educational institutions in the system of sustainable development of the region. International Journal of Sustainable Development and Planning, Vol. 18, No. 2, pp. 565-571. https://doi.org/10.18280/ijsdp.180226
[18] Kopytko, M., Sylkin, O. (2023). Modelling information support for combating corruption in the economic security management system of the state. Social and Legal Studios, 6(3), 60-66. https://doi.org/10.32518/sals3.2023.60
[19] Kwon, J. (2023). A study on ethical awareness changes and education in artificial intelligence society. Revue d'Intelligence Artificielle, Vol. 37, No. 2, pp. 341-345. https://doi.org/10.18280/ria.370212
[20] Kronivets, T., Yakovenko, O., Tymoshenko, Y., Ilnytskyi, M., Lasechko, S., Lasechko, M. (2023). The legal foundations for the utilization of artificial intelligence in educational processes. Relocoes Internacionais no Mundo Atual, 4(42): 686-702. https://doi.org/10.21902/Revrima.v4i42.6556
[21] Sylkin, O., Kryshtanovych, M., Petrovskyi, P., Sirant M. (2020) The Methodology of Hierarchical Ordering of Threats to Economic Security as the Basis for Educational and Practical Application for the Management of IT Sphere Enterprises, 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, pp. 639-642, doi: 10.1109/ACIT49673.2020.9208970.
[22] Huang, H., Hsin, C.T. (2023). Environmental literacy education and sustainable development in schools based on teaching effectiveness. International Journal of Sustainable Development and Planning, Vol. 18, No. 5, pp. 1639-1648. https://doi.org/10.18280/ijsdp.180535
[23] Kryshtanovych, M., Sakhanienko, O., Sylkin, O., Lypovska, S. (2022). Information support of public administration in the conditions of COVID-19. In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia), pp. 290-293. https://doi.org/10.1109/ACIT54803.2022.9913197
[24] Saleh, A.J., Alazzam, F.A.F., Rabbo Aldrou, K.K.A., Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. Journal of Security and Sustainability Issues, 10(1): 235-247. https://doi.org/10.9770/jssi.2020.10.1(17)
[25] Lim, S. (2017). Moral education in the age of artificial intelligence: From the perspective of consumer ethic. Journal of Ethics: The Korean Association of Ethics, 1(117): 89-116. https://doi.org/10.15801/je.1.117.201712.89
[26] Kryshtanovych, M., Bilyk, V., Hanushchyn, S., Sheremet, I., & Vasylenko, K. (2021). Modelling the ways to increase the creativity of psychology students as a basic factor in professional development. Creativity Studies, 14(1), 34-50. https://doi.org/10.3846/cs.2021.12571

Authors' Profiles

Myroslav Kryshtanovych: Doctor of Science in Public Administration, Full Professor, Professor of the Department of Pedagogy and Innovative Education, Work in Institute of Law, Psychology and Innovative Education. Work place: Lviv Polytechnic National University in Lviv. Areas of scientific interests: Public Administration, Intellectual Security, Modeling, Information Technology, Computer Systems.

Iryna Gavrysh: Doctor of Science in Pedagogy, Full Professor, Professor at the Department of Primary and Professional Education, Work in H.S. Skovoroda Kharkiv National Pedagogical University. Work place: Kharkiv, Ukraine. Areas of scientific interests: Education, Pedagogy, AI technology, Information Security.

Oleksandra Khltobina: Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Theory and Technology of Pre-school Education and Art Disciplines, Work in H.S. Skovoroda Kharkiv National Pedagogical University. Work place: Kharkiv, Ukraine. Areas of scientific interests: Education, Pedagogy, AI technology, Information Security.

Ihor Havrylov: Graduate student, Graduate student of the Department of Professional Education, Work Grigory Skovoroda University in Pereyaslav. Work place: Pereyaslav, Ukraine. Areas of scientific interests: Public Administration, Intellectual Security, Modeling, Information Technology, Computer Systems.

Yevhen Gren: Graduate student, Graduate student of the Department of Professional Education, Work Grigory Skovoroda University in Pereyaslav. Work place: Pereyaslav, Ukraine. Areas of scientific interests: Education, Pedagogy, AI technology, Information Security.

How to cite this paper: Myroslav Kryshtanovych, Iryna Gavrysh, Oleksandra Khltobina, Ihor Havrylov, Yevhen Gren, "The Effect of Threats from Using the Artificial Intelligence on the Educational Process in the Context of Information Security: A Methodological Approach to Modeling and Ordering Impact Levels", International Journal of Modern Education and Computer Science(IJMECS), Vol.16, No.5, pp. 21-32, 2024. DOI:10.5815/ijmecs.2024.05.02