Modern Economic-Legal Methods of Using Artificial Intelligence in An Educational Company: Information Technology to To Self-Development and Scientific Activity

Anna Pazieieva¹, Olesia Smolinska², Oksana Syniuk³, Olya Turytsya⁴ and Halyna Leskiv⁵

Abstract

The main goal of the article is to highlight the most dangerous threats of artificial intelligence in an educational company and to formulate economic and legal methods to counter them. The object of the study is the key information technologies of an educational company. The scientific task is to conduct a detailed study of the system for using information technologies in an educational company and the subsequent formation of the most effective economic and legal methods of countering threats in this area. The methodology includes methods of system analysis, graph theory, pairwise comparison and hierarchical analysis. As a result, a number of key threats to artificial intelligence in the educational company were identified, methods to counter them were formed. In addition, key countermeasures were identified. The study has limitations because it takes into account only a limited number of threats of the functioning of an individual educational company.

Keywords: Artificial Intelligence, Information Technology, Educational Companies, Economic and Legal Methods, Innovative Technologies, Pedagogy

INTRODUCTION

The emphasis of modern management of the use of artificial intelligence in an educational company is on the importance and state of the use of artificial intelligence in education, revealing key problems and trends in this area. The education sector is constantly evolving, and artificial intelligence plays a key role in this process, offering new opportunities for learning and management (Mazali, 2018).

The economic impact of artificial intelligence in education requires attention, because it can significantly increase the productivity of educational institutions, optimize costs and resources. At the same time, potential risks such as fewer jobs and increased inequality in access to education must be taken into account.

The legal aspect of the use of artificial intelligence in education includes issues of data confidentiality, intellectual property, responsibility for decision-making using artificial intelligence, and regulation of algorithms. It is important to ensure compliance with legal norms and moral standards in this area (Raisch, 2021).

Particular attention is paid to information technology in the context of artificial intelligence in education. The development of information technology contributes to the wider introduction of artificial intelligence into educational processes, opening up new opportunities for innovation and efficiency.

The issue of accessibility of artificial intelligence and information technology in various educational environments is important. Gaps in access to these technologies can exacerbate educational inequalities between different groups and regions.

It is also important to pay attention to international experience and practice in the use of artificial intelligence and information technologies in education in order to find effective ways to manage and integrate these technologies.

¹ «KROK» University, Kyiv, Ukraine
² Department of Philosophy and Pedagogy, Stepan Gzhytskiy National University of Veterinary Medicine and Biotechnologies, Lviv, Ukraine
³ Department of Management, Lviv National Environmental University, Lviv, Ukraine
⁴ Lviv Faculty of Food and Processing College of the National University of Food Technologies, Lviv, Ukraine
⁵ Lviv State University of Internal Affairs, Lviv, Ukraine; E-mail: galyna.levkiv.edu@gmail.com (Corresponding Author)
As a result, effective management that takes into account the economic, legal and social aspects of the use of artificial intelligence and information technology in education is key to improving the quality of education and promoting the development of society.

The development of information technology and artificial intelligence also raises the question of ethics and social responsibility. Discussing and developing ethical codes and standards of conduct for artificial intelligence in education is an important step to ensure transparency, fairness and responsibility in the use of these technologies (Miklosik et al. 2019).

So, the main goal of the article is to highlight the most dangerous threats of artificial intelligence in an educational company and to formulate economic and legal methods to counter them. The object of the study is the key information technologies of an educational company.

The structure of the article consists of an introduction, a literature review, a description of the methodology, a presentation of the research results, discussion and conclusions.

LITERATURE REVIEW

The study of modern literary sources is an important step in the formation of a management system using economic and legal methods for the effective use of artificial intelligence in an educational company. Analysis of current scientific works, articles, case studies and empirical studies provides valuable information about the latest trends, challenges and opportunities for using artificial intelligence in education.

So, Oreshkina et al. (2021) focuses on the digital educational environment as a key factor in the development of professional reflection of teachers. This study is important for understanding the impact of digital technologies, including artificial intelligence, on teacher professional development. It demonstrates how the integration of technology into the educational process can influence pedagogical approaches and teaching methods, which are a key aspect in the formation of a management system for the use of artificial intelligence in education.

In the context of the activities of the information technology sector, the study by Bazyluk et al. (2019) is interesting, since the authors tried to compare the institutional dynamics of the development of publishing and printing activities in Ukraine. This study highlights the importance of adapting institutional structures to modern technological changes. In the context of the application of artificial intelligence in education, this research can provide insights for managing institutional change and development.

In studies by Roztocki et al. (2019) and González-Zamar et al. (2019) the focus is on the role of information and communication technologies in socio-economic development. The study provides valuable insight into how ICT, including artificial intelligence, can influence the development of educational systems. It is important for assessing the potential economic and social benefits of integrating artificial intelligence into the educational process.

The work of Pradhan et al. (2018) explores the relationship between ICT infrastructure and economic growth. This research is important for understanding the impact of ICT investments, including artificial intelligence, on economic development. In the context of education, it provides insight into how investments in artificial intelligence can improve educational infrastructure and overall economic growth.

A study by Zhen et al. (2023) focuses on the impact of government subsidies on the development of public-private partnership projects in China. In the context of artificial intelligence in education, this research can provide valuable insights into funding and supporting such initiatives.

Similar is the Holmes (2020) and Luckin et al. (2022) studies, which analyzes the issue of artificial intelligence in education and its potential impact on learning processes. This resource is extremely important for understanding the potential of artificial intelligence in the educational field, including its opportunities, challenges and future impact. This study helps to better understand how artificial intelligence can transform the educational process and what management strategies need to be formed to effectively implement and use these technologies.
In Howe, Vial (2019) the authors explore the concept of digital transformation and its impact on strategic information systems. In the context of applying artificial intelligence to an educational company, this resource provides valuable insights on managing and adapting to digital change. The study helps to understand how organizations can effectively integrate emerging technologies, which is key to shaping management strategies.

A similar study by Alvarez et al. (2016) focused on processes of technology assimilation and divergence in times of crisis. This research is important for understanding the impact of economic crises on the adoption and adoption of technologies, including artificial intelligence. It can illuminate how economic factors influence strategic technology decisions in the education sector.

Boulay (2016) opinion on this topic is interesting too. So, the author is considering the use of artificial intelligence as a classroom assistant. This work provides perspective on the practical use of artificial intelligence in educational settings and its potential impact on the learning process. It is especially valuable for assessing the effectiveness of artificial intelligence in interaction with students and teachers.

Particularly noteworthy is the work of Sylkin et al. (2019), in which the authors explore the modeling of crisis management processes in the financial security system of an enterprise. In the context of managing artificial intelligence in an educational company, this source provides insights on risk management and crisis management.

So, the scientific task is to conduct a detailed study of the system for using information technologies in an educational company and the subsequent formation of the most effective economic and legal methods of countering threats in this area.

METHODOLOGY
The research methodology section examines four key methods: systems analysis, graph theory, paired comparison method, and hierarchical analysis, each of which is used to analyze key aspects of the application of artificial intelligence in an educational company.

System analysis is a method that allows us to consider complex systems by analyzing their elements, relationships and interactions. In the context of our study, systems analysis is applicable to study the interaction between artificial intelligence and various aspects of the educational system.

Graph theory is a mathematical method used to model the relationships between different objects or entities. It allows you to visualize the structure of systems, showing how elements interact with each other. This is especially useful for identifying key nodes and relationships in a system. The advantage of graph theory is its ability to visualize and simplify complex structures.

The paired comparison method is used to organize and rank different elements or options according to certain criteria. In this study, it will be applied to assess and prioritize various types of threats associated with the integration of artificial intelligence into the educational system. This helps determine which aspects require more attention and resources.

Hierarchical analysis is a technique that allows to break a complex problem into smaller, more manageable parts by organizing it into a hierarchical structure. In the context of our study, it can be used to structure and analyze different risk management strategies. This method allows to determine which strategies are most effective for solving specific problems.

Thus, the combination of these four methods creates a complete and effective methodological basis for researching and solving complex problems associated with the implementation and management of artificial intelligence in an educational company. The use of various methods allows you to deeply analyze and identify key challenges and opportunities, as well as develop strategies for effectively managing them.

RESULT AND DISCUSSION
In the context of planned methods, including systems analysis, graph theory, paired comparison and hierarchical analysis, our research identified nine key threats associated with the use of artificial intelligence in the educational field. These threats cover a wide range of issues, from data privacy and security issues to technology dependence, ethical challenges, impact on the teacher's role, the accuracy and objectivity of HI decisions, limitations on personal development, reduced creativity, and problems in assessment and feedback. These identified threats were carefully analyzed using specified methods to provide a deep understanding of potential risks and develop effective strategies to counter them in the education sector. 

So, we have identified nine key threats to the use of artificial intelligence in an educational company. For further convenience, each of the threats was designated by a symbolic name (Tn)

T1 - Impact on the teacher's role. The integration of AI in education could change the traditional role of teachers, focusing on the use of technological tools instead of direct teaching. This can reduce the importance of teaching skills and personal interaction between teacher and student.

T2 - Inequality in access to technology. Widespread adoption of AI in education may lead to inequalities in access to quality education, as not all students and schools have the same access to the necessary technological resources. This could lead to a stratification of educational opportunities, where students from less affluent areas or schools are left out of reach of the benefits provided by AI.

T3 - Technology addiction and skill loss. Increasing dependence on AI and other information technologies in the educational process may lead to a loss of traditional learning skills and teaching methods. This may include a decrease in the ability to think critically and solve problems without the help of technology.

T4 - Ethical issues and abuses. The use of AI in education raises moral questions for society, such as the potential misuse of technology to manipulate or control students. This is relevant to information technology because a strict ethical framework is required for the use of AI in education.

T5 - Data privacy and security. The use of artificial intelligence (AI) in education can lead to risks associated with storing and processing large amounts of personal data of students and teachers. This is relevant to information technology, since insufficient privacy and data security can lead to the leakage of sensitive information, which negatively affects the privacy of individuals and institutional reputation.

T6 - Accuracy and objectivity of AI solutions. AI systems used in education may have built-in warnings or errors that affect the quality of education and the objectivity of the assessment. Improperly configured algorithms can lead to inaccurate training recommendations or assessments.

T7 - Reduced personal development. Over-automation of the learning process by AI may limit the opportunities for students to develop interpersonal skills and critical thinking. This is important because education not only imparts knowledge but also contributes to the development of a complete personality.

T8 - Limit creativity and innovation. AI can limit creativity in the learning process by relying on algorithmic decisions and standardization. This can lead to decreased innovativeness and originality in solving problems and generating new ideas.

T9 - Difficulties in assessment and feedback. AI may be limited in its ability to provide expert assessment and feedback, which is critical to the learning process. Automated systems can take into account the individual characteristics of students, their learning style and emotional state, which can affect the quality and effectiveness of learning.

Figure 1 shows a diagram of the key threats to the use of artificial intelligence by an educational company. Difficulties in assessment and feedback
In our work, we sought to improve the methodology for assessing threats arising from the use of information technology and artificial intelligence in educational companies. To achieve this goal, we turned to the method of systems analysis and graph theory. Although this approach is widely used in many fields, its use for AI threat analysis in the education sector is quite new. Thus, our research contributes to the development of methods for assessing and managing threats arising in this area.

The list of detected threats is presented in the form of a set, the elements of which have interconnections. To visually demonstrate these connections, we constructed a graph (see Figure 2).
After constructing the connection graph, the next step is to form a binary dependency matrix. The essence of a binary matrix is to create a structured image of the relationships between different identified threats, where each element of the matrix represents the presence (value “1”) or absence (value “0”) of dependence between pairs of threats (Table 1).

Table 1: Binary dependency matrix of threats to the use of artificial intelligence in educational companies

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
<th>T8</th>
<th>T9</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>value:0</td>
<td>value:0</td>
<td>value:1</td>
<td>value:1</td>
<td>value:0</td>
<td>value:1</td>
<td>value:1</td>
<td>value:0</td>
<td>value:1</td>
</tr>
<tr>
<td>T2</td>
<td>value:0</td>
<td>value:0</td>
<td>value:1</td>
<td>value:1</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T3</td>
<td>value:0</td>
<td>value:1</td>
<td>value:0</td>
<td>value:1</td>
<td>value:0</td>
<td>value:1</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T4</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T5</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T6</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T7</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T8</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
<tr>
<td>T9</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
<td>value:0</td>
</tr>
</tbody>
</table>

Source: own analysis

So, in this matrix, rows and columns correspond to different threats. If one threat potentially affects another, a “1” is placed in the corresponding matrix cell. If there is no such impact, the cell is filled with "0". This allows you to visualize and systematize the complex relationships between threats, which is critical for understanding the overall picture of the risks that arise when introducing artificial intelligence into the educational process.

Thanks to the binary dependency matrix, you can effectively assess which threats have the greatest impact on the system as a whole and develop strategies to minimize these risks. Using this approach is important for developing comprehensive and effective risk management mechanisms in educational companies using artificial intelligence.

The calculated dependency matrix forms the necessary basis for determining the content of the reach matrix.
A reach matrix is an important analytical tool used to identify and analyze the relationships between different elements in a network or system. This allows to determine whether one threat can lead to another, or whether there is a direct or indirect relationship between them (Table 2).

**Table 2: Binary dependency matrix of threats to the use of artificial intelligence in educational companies**

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
<th>T8</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>T2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>T3</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>T4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>T5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>T6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>T7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>T8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: own analysis

Formation of the reach matrix includes data analysis using the dependency matrix. This allows us to identify not only direct, but also indirect interactions between threats, which is important for understanding the depth and complexity of the risks that an educational company faces. Taking into account the data displayed in the previously constructed graph (Figure 3) and the results obtained from the reachability matrix (Table 1), the order of the threat hierarchy is established. This is done by creating an iterative table (Table 3), where the column S(Ti) indicates the node numbers that can be reached, the column P(Ti) displays the set of previous nodes, and the third column determines whether a certain condition is satisfied for each of the threats.

**Table 3: Binary dependency matrix of threats to the use of artificial intelligence in educational companies**

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
<th>T5</th>
<th>T6</th>
<th>T7</th>
<th>T8</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>1, 3, 4, 6, 9</td>
<td>2, 4</td>
<td>2, 3, 4, 6</td>
<td>4</td>
<td>4, 5</td>
<td>5, 6</td>
<td>2, 7</td>
<td>6, 8, 9</td>
</tr>
<tr>
<td>S(Ti)</td>
<td>1</td>
<td>2, 3, 7</td>
<td>1, 3</td>
<td>1, 2, 3, 4</td>
<td>5</td>
<td>6, 8, 9</td>
<td>1, 7</td>
<td>3, 8</td>
</tr>
<tr>
<td>P(Ti)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

At the lowest level of the hierarchical structure of external threats is threat T1, which satisfies a certain condition. The next step involves removing the first row and corresponding numeric values from other rows, after which a new iterative table is formed. This methodological approach, using sequentially calculated iteration tables, made it possible to create a hierarchical model reflecting the importance of the influence of external threats on investment security. This model is presented in Table 4.

**Table 4: Hierarchical threat model for a system using artificial intelligence in an educational company**

<table>
<thead>
<tr>
<th>Level</th>
<th>Threat</th>
<th>Threat vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 6</td>
<td>T1</td>
<td>T3</td>
</tr>
<tr>
<td>Level 5</td>
<td>T5</td>
<td></td>
</tr>
<tr>
<td>Level 4</td>
<td>T9</td>
<td>The growing importance of influencing the system of using artificial intelligence and information technology in an educational company (From Level 1 to Level 6)</td>
</tr>
<tr>
<td>Level 3</td>
<td>T2</td>
<td>T8</td>
</tr>
<tr>
<td>Level 2</td>
<td>T5</td>
<td>T7</td>
</tr>
<tr>
<td>Level 1</td>
<td>T1</td>
<td></td>
</tr>
</tbody>
</table>

Source: own analysis
Using our chosen methods, including systems analysis, graph theory, pairwise comparison, and hierarchical analysis, we found that among the various threats associated with the use of artificial intelligence in educational companies, T4 “Data Privacy and Security” and T5 “Ethical Issues” have the greatest impact and abuse. These threats turned out to be key in the context of the potential impact on the efficiency and security of information technology in an educational company.

First of all, the threat that has the greatest impact is T4 "Data Privacy and Security"

One of the key responses to data privacy and security threats is to develop and implement strong privacy and data security policies. This includes the use of modern encryption technologies, installation of reliable firewalls and intrusion detection and prevention systems. It is also important to provide regular training to staff on the basics of cybersecurity and establish procedures to ensure that all educational staff are aware of the potential risks and know how to act in the event of a data security breach.

The second key threat is T5 "Ethical Issues and Abuses". Regarding moral issues and abuses, it is necessary to develop and implement clear ethical norms and standards for the use of artificial intelligence in education. This includes creating institutional frameworks that regulate the use of information technology and set boundaries for data collection and analysis. It is also important to involve ethics experts, lawyers and other professionals to ensure that the technologies and techniques developed meet high ethical standards.

As a result of our research, we were able to identify and assess the key threats associated with the use of artificial intelligence in educational companies. In particular, we found that aspects such as data privacy and security and ethical issues and abuse have the most significant impact. Thus, our study not only contributes to a better understanding of risks, but also provides practical recommendations for effectively managing these risks in the education sector.

**DISCUSSION**

Comparing our research results with existing scientific work and advances is a key element in enhancing the quality and relevance of our work. This process not only reveals the unique contributions our research makes to the field of artificial intelligence in education, but also contributes to a deeper understanding of the current state of this rapidly developing field.

For example, Harris and Jones (2018) analyze why context matters when implementing educational reforms and policies. They note the diversity of educational systems and the need to adapt reforms to local conditions. In the context of our study, this is important for understanding how different educational contexts may influence the adoption and use of artificial intelligence. Our study adds to this analysis by demonstrating how specific features of artificial intelligence and information technology can be adapted to different educational environments.

The work of Pedro et al. (2018) the authors provide a critical analysis of the integration of mobile learning into formal educational contexts. They look at the challenges and benefits of using mobile technology in learning. While we shape the strategy for introducing artificial intelligence into the educational process, ensuring that technological solutions are effectively integrated into the learning environment.

At the same time, Awe, Church (2020) focuses on project flexibility and creativity, analyzing the role of training in improving project performance. In our study, we extend these findings to understand the importance of training and education in the implementation of artificial intelligence in the educational process, especially in terms of increasing flexibility and creativity in management and teaching.

Wiesboeck, Hess’s (2020) study examines the integration of digital innovation in organizations. They explore how companies are adapting to digital technologies and the challenges they face. While our research focuses on how educational institutions can adapt to the use of artificial intelligence, ensuring effective integration and use of these technologies.

Baesu, Bejinaru (2020) explores knowledge management strategies for leadership in a digital business environment. Their work focuses on the general principles of knowledge management and their application in
Modern Economic-Legal Methods of Using Artificial Intelligence in An Educational Company: Information Technology to To Self-Development and Scientific Activity

a business context. Our research is different in that we will focus on the application of knowledge management to implement and optimize artificial intelligence in the educational field, providing more specific and targeted strategies for educational leaders.

At the same time, Ertmer, Otternbreit-Leftwich (2019) focus on teachers' change in technology and the interaction of knowledge, confidence, beliefs and culture. Our research extends this analysis by examining how these factors influence the adoption and integration of AI specifically in the educational process, providing a deeper understanding of the specific challenges and opportunities presented by the use of these advanced technologies. Fernández-Gutiérrez, et al. (2019) research appears to be analyzing the impact of ICT use on student outcomes. Our research complements this analysis by focusing on a specific aspect of ICT — artificial intelligence — and its potential to enhance learning and improve learning outcomes, providing additional context and depth to understanding the role of technology in education.

Volchik's (2020) study examines institutional traps in the education and science sector under conditions of optimization. This work is important in identifying institutional constraints, but our research differs in that it focuses on developing strategies to counteract these pitfalls, particularly in the context of integrating artificial intelligence into the educational process, making our approach more specific and focused on practical problem solving.

Having compared the results of our research with existing scientific works and achievements in the field of application of artificial intelligence in education, we can claim that our research is highly relevant and has significant scientific value. The relevance of our research is reinforced by the constant development and integration of artificial intelligence into various areas of education; its scientific value is due to in-depth analysis and development of practical recommendations that can be applied in educational management. Therefore, our study not only contributes to academic enrichment in this field, but also provides valuable guidance for practitioners seeking to optimize the use and management of artificial intelligence in the educational process.

CONCLUSION AND RECOMMENDATION

In conclusion to the study, which focuses on the current state of management using economic and legal methods for the application of artificial intelligence in an educational company, special attention should be paid to the role of information technology and the identification of potential threats. Artificial intelligence as an instrumental component of modern education provides new opportunities for automation, personalization of learning and increasing the efficiency of educational processes, but also poses new challenges for management in the integration and use of these technologies.

The use of artificial intelligence in educational institutions requires careful consideration of economic and legal aspects, including financing, budgeting, technology infrastructure costs, and compliance with legal regulations and standards. Information technologies offer significant opportunities for the development of education, but they carry risks associated with data security and dependence on technological systems. Therefore, it is critical to develop and implement information systems security strategies that include cybersecurity measures, training staff and students in information technology security fundamentals, and developing incident response plans.

As a result of using methods of system analysis, graph theory, paired comparison method and hierarchical analysis, the key threats that artificial intelligence can pose in an educational company have been identified. These threats include data privacy concerns, technology dependency risks, change management challenges, and the need to adapt curriculum. Accordingly, key economic and legal methods have been proposed to counter these threats, including developing comprehensive data protection strategies, improving the legal framework for regulating and monitoring artificial intelligence in the education sector, and establishing effective risk management mechanisms.

As a result, a number of key threats to artificial intelligence in the educational company were identified, and on the basis of this, economic and legal methods to counter them were formed. In addition, key countermeasures were identified. The study has limitations because it takes into account only a limited number of threats and realities of the functioning of an individual educational company.
REFERENCES


Modern Economic-Legal Methods of Using Artificial Intelligence in An Educational Company: Information Technology to Self-Development and Scientific Activity


