A Model for Financing the Process of Education Informatization, Taking into Account Computer Security within the Framework of a Differential Quality Game

Arkadii Chikrii [1], Kaiyrbek Makulov [2], Volodimir Malyukov [1], Berik Akhmetov [2], Valerii Lakhno [3], Inna Malyukova [4], and Bagdat Yagaliyeva [5,6,*]

[1] Department of Optimization of Controlled Processes of the V. M. Glushkov, Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2] Department of Computer Science, Caspian University of Technology and Engineering Named after Sh. Yessenov, Aktau, Kazakhstan
[3] Department of Computer Systems and Networks, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
[4] Rating Agency "Expert-Rating", Lead Analyst, Kyiv, Ukraine
[5] Global Education and Training, School at Illinois, University of Illinois at Urbana Champaign, Champaign, Illinois, USA
[6] Department of Cybersecurity, Information Processing and Storage, Satbayev University, Almaty, Kazakhstan
Email: g.chikrii@gmail.com (A.C.); kaiyrbek.makulov@yu.edu.kz (K.M.); volod.malyukov@gmail.com (V.M.); berik.akhmetov@yu.edu.kz (B.A.); lva964@nubip.edu.ua (V.L.); imalyukova82@gmail.com (I.M.); bagdaty@illinois.edu, b.yagaliyeva@satbayev.university (B.Y.)
*Corresponding author

***Abstract*—This article proposes a game-theoretic model for financing education informatization, incorporating Cyber Security (CS) considerations within a university context. The model formalizes the financial interactions between stakeholders, addressing the critical interdependence between educational quality and cybersecurity. This interdependence necessitates optimized resource allocation to establish a secure and innovative educational environment. The core challenge investigated is the strategic balance between investments in digitalization and the costs of associated information security measures. The novelty of our approach lies in applying a differential quality game with a bilinear structure, where the participants' financial states are governed by a system of differential equations. Classical methods for solving linear differential games are inapplicable here, as the bilinear structure prevents the use of the Cauchy formula to solve the system. Furthermore, the positional differential game approach is also unsuitable, as the model permits the use of non-measurable controls by an opponent. These mathematical challenges underscore the work's significance, contributing not only as a tool for CS policy but also through its theoretical advancements. Within this framework, the model identifies player preference sets and optimal strategies, findings which are validated through a computational experiment. The visualization of the preference set for the first player—the Computer Security Center (CSC)—demonstrates the model's practical utility in resolving financing dilemmas for education informatization amid cybersecurity constraints. The study's impact lies in providing a robust analytical tool for developing optimal resource allocation strategies. This contributes significantly to the sustainable development of Higher Education (HE) systems navigating digital transformation and escalating cyber threats.**

***Keywords*—higher education, informatization, cybersecurity, game theory, scenarios, resources, optimal strategy**

I. Introduction

The quality of Higher Education (HE) is a cornerstone of national progress, providing the foundation for training highly qualified specialists who will drive the sustainable development of the economy and society in the Republic of Kazakhstan (RK). In an era marked by rapid digitalization and the integration of Information Technologies (IT) into educational processes, Higher Education Institutions (HEIs) in Kazakhstan face new challenges, particularly those related to Cyber Security (CS) and information protection.

The relevance of this study is underscored by the growing need for innovative approaches to enhance the quality of HE amidst the digital transformation of Kazakhstan's economy. While this transformation creates new opportunities for education, it also introduces significant risks that demand careful analysis and strategic management.

Manuscript received June 12, 2025; revised June 26, 2025; accepted September 2, 2025; published December 12, 2025.

To address these challenges, we model the interaction between two key players in the HE system: the Computer Security Center (CSC), which possesses resources dedicated to ensuring cybersecurity. For instance, the center may have a portfolio of security tools whose deployment and maintenance require financial investment. The second player is the Education Financing Center (EFC), such as a Ministry of Education, which focuses on improving education quality through the adoption of IT solutions, including cloud technologies, gamification, and other innovations.

The activities of the CSC and EFC are intrinsically linked. A clear correlation exists between "digitalization" (the integration of IT in education) and the need to strengthen CS in universities. As more resources are invested in digitalizing education, the demand for enhanced CS measures grows accordingly.

Typical scenarios in Kazakhstani HEIs illustrate this interdependence:

- The introduction of distance learning platforms (e.g., Moodle, Canvas) requires robust protection for personal data and secure online examination processes.
- The use of cloud storage for educational materials increases the risk of Unauthorized Access (UA), necessitating measures like multi-factor authentication and data encryption.
- The expansion of campus Wi-Fi networks enhances resource accessibility but also requires modern firewalls and intrusion detection systems to counter potential cyberattacks.

Conversely, robust cybersecurity enables and encourages further IT adoption, creating a positive feedback loop that enhances the quality of education. For example:

- A secure environment allows for the safe implementation of virtual laboratories and simulators, expanding practical training opportunities.
- Advanced data protection facilitates the development of extensive digital libraries and research databases, improving information accessibility.
- A reliable CS infrastructure enables secure participation in international educational collaborations and exchange programs.
- Secure systems support innovative assessment methods, such as adaptive testing, improving objectivity and efficiency.

Given this dynamic relationship, this study employs a differential quality game to model and evaluate the complex interactions between IT adoption and CS enhancement. The application of game theory to this problem helps identify optimal resource allocation strategies, balancing the need for innovative educational development with the imperative of ensuring security.

The application of game theory is well-established across various economic and social fields. In this specific context, the application of methods for solving bilinear differential quality games is a natural fit. Processes such as maintaining cybersecurity within an educational system are qualitatively described by bilinear differential game models, as the underlying resource allocation procedure dictates this bilinear dynamic. The bilinear nature of the dynamics necessitates specialized solution methods, which constitutes the mathematical novelty of this work and contributes to advancing the toolkit for bilinear differential games.

The significance of this problem lies not only in the rapid digitalization of HE in Kazakhstan but also in the escalating cybersecurity risks that accompany it. Given constraints on resources and the need for balanced decision-making, optimal fund allocation between IT infrastructure development and university cybersecurity measures is critical for the sustainable growth of Kazakhstan's HE system. Employing game theory provides a powerful analytical framework for crafting effective strategies that align with digital transformation goals while mitigating emerging cyber threats—an approach with potential applicability in other national contexts.

II. Literature Review

A significant body of research has been devoted to cybersecurity issues in universities and other educational institutions. A number of studies also explore the relationship between the quality of education and the provision of cybersecurity in these institutions.

For instance, AlDaajeh *et al*. [1] examine the impact of national cybersecurity strategies on the development of education in the field. They analyze how government initiatives and policies can enhance curricula, train specialists, and raise overall awareness of cyber threats. The study also highlights the importance of integrating cybersecurity into educational systems to ensure national security.

Lehto [2] investigates approaches to education and research in cybersecurity at universities and applied sciences institutions in Finland. The study analyzes existing curricula, teaching methods, and research initiatives, emphasizing the need to train specialists in cybersecurity. While the research identifies challenges and prospects in developing cybersecurity within Finland's education system, it is primarily analytical and does not address the relationship between investments in university cybersecurity and education quality.

Alhumud *et al*. [3] present a more compelling approach, using a quality management framework to assess the cybersecurity level in Saudi Arabian universities. The study identifies the strengths and weaknesses of current cybersecurity practices in educational institutions and provides recommendations for improvement. The authors emphasize the importance of integrating quality management principles into cybersecurity practices to enhance overall security in education.

Elsawy and Ahmed [4] investigate the use of the Blackboard e-learning system, focusing on the relationship between education quality and cybersecurity. They discuss how the platform supports educational processes while addressing risks associated with cyber threats. The study

offers recommendations to improve data security and user protection during online learning. However, it lacks a mathematical justification for its conclusions.

In terms of using game theory to assess university development strategies and enhance educational processes, several studies are noteworthy.

For example, Selim [5] plies game theory to analyze the education market in Egypt, exploring interactions between students, educational institutions, and government agencies. The study examines how competition and cooperation influence the quality and accessibility of education. It also discusses strategic decisions that can improve educational outcomes and optimize resource allocation.

Beltadze [6] considers the application of game theory in higher education and educational processes. The study analyzes how game theory models can improve interactions between students, teachers, and institutions, optimizing learning strategies and enhancing the efficiency of education. However, it does not address the relationship between these strategies and cybersecurity challenges.

Ekinci *et al*. [7] combine Multi-Criteria Decision-Making (MCDM) with game theory to propose a method for selecting strategies in higher education. This approach helps institutions evaluate and implement effective strategies based on various criteria and interactions between stakeholders. The study focuses on improving management and resource optimization, as well as enhancing institutional competitiveness. Nevertheless, it does not address the correlation between education quality and university cybersecurity.

Similarly, Correa and Gruver [8] apply game theory to analyze the interaction between teachers and students in the educational process. The study expands the economic theory of education by examining how the decisions and strategies of both parties affect learning outcomes and education quality. While the research underscores the importance of understanding these interactions to improve efficiency and resource optimization, it does not consider the relationship between education quality and cybersecurity.

As evident from these studies and other works we have reviewed, there is a noticeable gap in research systematically addressing the modeling of financial processes for the informatization of education, particularly with consideration of computer security [9–12]. This gap highlights the relevance of our research.

It should be noted that in studies [13–15], new approaches aimed at improving the quality of education have been proposed, based on the application of game theory ideology, particularly gamification—that is, the inclusion of game mechanics and aesthetics, as well as cognitive and behavioral aspects associated with games, into non-game educational content. These approaches can be applied to the problem considered in this study as part of the toolkit for enhancing the quality of education, which requires financial support to address the interrelated issue of improving education quality and ensuring an acceptable level of cybersecurity.

In the context of international scholarship, the financing of digital transformation in education, with particular consideration of cybersecurity threats, has been the subject of active research in the European Union, the United States, and various Asian countries [16, 17]. For instance, several contributions [18, 19] focus on the mechanisms of balancing resource allocation between IT-driven innovations and cybersecurity measures in higher education institutions in the United Kingdom and other jurisdictions [20], where these issues are addressed within the framework of stringent regulatory regimes for data protection, such as GDPR and PIPEDA. In China and South Korea, the concept of a ‘dual financing contour’ is applied, whereby resources for cybersecurity and digitalization are allocated in parallel, ensuring the sustainable development of IT infrastructure in higher education institutions [21–23]. Findings from the comparison of contemporary approaches with the model proposed in this article highlight its potential applicability across different national contexts, while preserving the integrity of its mathematical foundation [24–26].

Taken together, the above considerations indicate that the subject of our investigation is of significant relevance.

All of the above indicates that the topic of our research is highly relevant and that our work addresses a clear gap in the existing literature by integrating financing, cybersecurity, and education quality within a formal game-theoretic model.

III. Research Objective and Tasks

The primary objective of this research is to develop and refine mathematical models that form the basis for a decision support system aimed at optimizing the allocation of resources—financial, intellectual, personnel, and technical—between the processes of education informatization and ensuring cybersecurity within higher education institutions.

The following tasks were undertaken to achieve the research objective:

A. Development of a Game Theory Model

A differential quality game model was formulated to identify the optimal strategies for the key players. The study includes deriving an analytical solution to the game and analyzing the conditions under which the players achieve their objectives when employing optimal strategies.

B. Conducting a Computational Experiment

A computational experiment was conducted to test and validate the model, the results of which are presented in the following section.

The problem examined in this study is effectively addressed through the use of a bilinear differential quality game framework, as this approach allows for the inclusion of numerous factors relevant to the issue. Specifically, it takes into account the allocation of financial resources, the level of information available to the players, the continuity of the process, and other related aspects.

IV. Materials and Methods

The quality of Higher Education (HE) is a cornerstone of national progress. While global digitalization offers innovative opportunities to enhance, HE quality, it also introduces additional risks, as evidenced by the literature analysis. These risks demand careful analysis and management. To address this, we propose modeling the interaction between two key players in the HE system, responsible for resource allocation between education informatization and ensuring cybersecurity in universities.

In our model, various types of resources—financial, human, intellectual, technical, and organizational—are converted into a single financial equivalent. This simplification facilitates the creation of a universal resource allocation model and enables quantitative analysis. However, we acknowledge the limitations of this approach, as certain qualitative aspects of resources may not be fully captured in financial terms. Therefore, interpreting the model's results will require considering the qualitative characteristics of resources and their specific applications.

This section focuses on the methodological foundation for developing and analyzing the game-theoretic model of resource allocation between education informatization and cybersecurity. The approach is grounded in the theory of differential games, which allows for modeling dynamic interactions and strategies for key players.

The problem arises from the need to balance the competing interests of the Cyber Security Center (CSC) and the Education Financing Center (EFC), as described in detail in the Introduction. While the problem formulation provides the context, the methods presented here aim to solve the problem using mathematical tools and computational experiments. Emphasis is placed on model construction, determining optimal strategies, and validating these strategies through a series of experiments.

The quality of HE plays a key role in the progress of any state. Innovative approaches to improving the quality of HE in the context of global digitalization not only open up new opportunities but also create, as the analysis of the literature has shown, additional risks that require careful analysis and management. Recognizing these risks and opportunities, we propose considering the interaction of two key players in the HE system. These players are responsible for allocating resources between the processes of education informatization and ensuring computer security in universities. Within our model, we reduce various types of resources (financial, human, intellectual, technical, and organizational) to a single financial equivalent. This simplification allows for the creation of a universal resource allocation model and facilitates quantitative analysis. However, we acknowledge the limitations of such an approach and recognize that some qualitative aspects of resources may not be fully reflected in the financial assessment. Therefore, when interpreting the model results, it will be necessary to additionally consider the qualitative characteristics of resources and the specifics of their application.

A. Problem Statement

There are two players: The first player is the Cybersecurity Center (CSC). It has resources aimed at ensuring cybersecurity; for example, it can be assumed that the center has a set of cybersecurity tools for which resources must be allocated. These tools can be called the CSC's technological strategies. The second player is the Education Financing Center (EFC). Its main task is to improve the quality of education, including through the introduction of IT into the learning process, such as cloud technologies and other innovative solutions. It is assumed that the second player has a set of tools (its technological strategies) that it can use to improve the quality of education.

For example, consider a small list of player strategies, each of which will require corresponding resources that can ultimately be reduced to the dimension of financial Resources (RES) with the limitations that were discussed above; see Table I.

Interdependence in the financing of cybersecurity and education informatization is a complex dynamic mechanism in which one player's resources influence the actions and needs of the other. For example, funding the CSC directly stimulates additional investments in the informatization of the educational process. This is because the more funds are directed towards introducing IT into education, the more pressing cybersecurity issues become, and consequently, the more resources are required to address them effectively.

On the other hand, a high level of cybersecurity creates attractive conditions for the introduction of new IT. Thus, increasing investments in cybersecurity not only protects existing university information systems but also serves as a powerful incentive for further innovation. This, in turn, contributes to improving the quality of educational services in universities. This interdependence of financing processes leads to a conflict of interest between the players, as one of them often finds itself unable to meet the financial demands of the other. A shortage of resources—especially financial ones—can block the implementation of their own technological strategies.

In this regard, we use the term "resource" (RES) to denote all the necessary funds allocated by the players. The conflicting relationship between the CSC and the Education Financing Center (EFC) forms the basis for applying game theory, namely an antagonistic game, to the problem of finding optimal strategies for the participants. We model this interaction as a differential quality game, which allows us to account for changes and the adaptation of player strategies depending on current conditions. The interaction between the players occurs continuously over time, emphasizing its dynamic nature. As previously mentioned, the first player (CSC) allocates funding to its technological strategies aimed at protecting cybersecurity, while the second player (EFC) funds its strategies aimed at improving the quality of education through the introduction of IT. The EFC's investment in its technological initiatives, in turn, requires additional funds from the CSC to ensure their protection, creating a closed loop of mutual dependencies and financial obligations.

TABLE I. EXAMPLES OF POSSIBLE PLAYER STRATEGIES

Players	Player strategies	No. of strategy	Name of the strategy	Description
Player 1	Cybersecurity Center	1	Network Activity Monitoring	Using tools for continuous monitoring and analysis of traffic in a university network and its information systems to identify anomalies and threats
		2	Security Audit	Conducting regular checks of the university's systems for vulnerabilities and weaknesses for their subsequent elimination
		3	Security Policy Development	Creating and implementing a clear data security policy within the university's information systems, including access rules and data processing procedures
		4	AI Integration into University Security Systems	Implementing Artificial Intelligence Technologies for Automated Threat Analysis and Incident Response in Higher Education Institution Information Systems
		5	And others	
	Education Financing Center	1	Cloud technology implementation	Using cloud platforms for storing and processing educational materials, which ensures accessibility and flexibility in organizing the educational process
		2	Integration of Learning Management Systems (LMS)	Implementing learning management systems to simplify planning and assessment of the quality of the educational process at the university
		3	Creation of high-quality interactive learning materials	Developing high-quality multimedia and interactive resources that adapt to the knowledge level and learning pace of each student. As well as educational materials that are accessible to students with diverse needs, including those with physical or cognitive limitations
		4	Training Teachers in New IT Solutions	Organizing courses for university professors on the use of modern IT technologies in teaching
		5	And others	
Player 2	Cybersecurity Center	1	Network Activity Monitoring	Using tools for continuous monitoring and analysis of traffic in a university network and its information systems to identify anomalies and threats
		2	Security Audit	Conducting regular checks of the university's systems for vulnerabilities and weaknesses for their subsequent elimination
		3	Security Policy Development	Creating and implementing a clear data security policy within the university's information systems, including access rules and data processing procedures
		4	AI Integration into University Security Systems	Implementing Artificial Intelligence Technologies for Automated Threat Analysis and Incident Response in Higher Education Institution Information Systems
		5	And others	
	Education Financing Center	1	Cloud technology implementation	Using cloud platforms for storing and processing educational materials, which ensures accessibility and flexibility in organizing the educational process
		2	Integration of Learning Management Systems (LMS)	Implementing learning management systems to simplify planning and assessment of the quality of the educational process at the university
		3	Creation of high-quality interactive learning materials	Developing high-quality multimedia and interactive resources that adapt to the knowledge level and learning pace of each student. As well as educational materials that are accessible to students with diverse needs, including those with physical or cognitive limitations
		4	Training Teachers in New IT Solutions	Organizing courses for university professors on the use of modern IT technologies in teaching
		5	And others	

Let's assume that $i-$ is a technological strategy of the EFC that leads to the need for the CSC to spend resources in the amount of ρ_j^1. Then, $j-$ is a technological strategy of the CSC that leads to a cost of resources for the EFC in the amount of ρ_j^1. Let's give an example.

Suppose the EFC wants to introduce a new online learning system (this $i-$ is the technological strategy of the EFC). The EFC invests in a platform for conducting online courses. The introduction of this system will require additional CS measures; accordingly, the CSC needs to allocate additional resources ρ_j^1 $(i-)$ to strengthen the protection of the personal data of students and teachers, as well as to protect against DDoS attacks on online learning servers.

In response, the CSC introduces a multi-factor authentication system (this $j-$ is the technological strategy of the CSC). The introduction of this CS system, in turn, will allow the EFC to expand the functionality of the online platform, including conducting online exams and attracting more foreign students due to the increased level of data protection, as well as reducing the risks of financial losses from possible cyberattacks. However, this will require additional investments from the EFC ρ_j^1 $(j-)$ in the development and adaptation of the educational platform for new opportunities provided by the increased level of CS.

Thus, one can clearly see in this small example how the actions of one center (the introduction of a new technology) lead to the need for additional investments from the other center, and vice versa, which, in fact, illustrates the relationship and mutual influence of the strategies of both players in the proposed model.

Let us denote by p_{ij}^1 the ratio ρ_i^1 / ρ_j^2, and by p_{ij}^2 the ratio ρ_j^2 / ρ_i^1. If $\rho_i^1 = 0$ is very large for some i and j, or $\rho_j^2 = 0$ is very large for some j, then such strategies are excluded from consideration.

Let's assume that S_1 is a matrix of size $n \times m$, consisting of elements s_{ij}^1. The number of rows of the matrix S_1 is the number of technological strategies of the EFC. In the matrix S_1, the number of each row is the technological strategy of the EFC. The column numbers of

S_1 are the technological strategies of the CSC. Then S_2 is a matrix of size $n \times m$. In S_2, the row numbers are the technological strategies of the CSC. The column numbers of S_2 are the technological strategies of the EFC. We obtain that the elements s_{ij}^2 mean that they are located in the $j-$оù row and $i-$ом column.

Let us denote by p_{ij}^1 the ratio, and by the ratio. If it is very large for some and j or is very large for some, then such strategies are excluded from consideration.

To make further calculations more compact, we introduce the following notations:

δ_j $(j=1,...,m)-$ Elements of a diagonal matrix Ξ order m: $\delta_j \geq 0, \sum_{j=1}^{m} \delta_j = 1$. Matrix Ξ characterizes the 'structure' of the EFC's resources.

δ_j represents a portion $j-$ of the CSC's resource set, which is transformed into $j-$ a component of the same size within the EFC's resource set. What does this situation correspond to? If we have a CSC resource set $(w_1,...,w_n)$ of size $j-$, then the y-component of the EFC's resource set of the same magnitude is transformed into a CSC resource set equivalent to $\delta_j \cdot (w_1,...,w_n)$.

θ_j $(j=1,...,n)-$ The elements of the diagonal matrix Ψ are ordered by n: $\theta_j \geq 0, \sum_{j=1}^{n} \theta_j = 1$: XX:X. Matrix Θ describes the structure of the CSC's resource set. Each element in θ_j represents a share $j-$ of the EFC's resource set, which is transformed into a corresponding component $j-$ in the CSC's resource set.

This means that if there is a resource set in the EFC represented by $(g_1,...,g_m)$, then in the j component, the resource set magnitude of the CSC is transformed to match the resource set magnitude of the CFO, also represented by $\theta_j \cdot (g_1,...,g_m)$.

We assume that there exists a set of resources, $w=(w_1,...,w_n)$, available to the Central Design Bureau (CDB) for operation. $(S_1 \cdot w)$ represents $m-$ a multidimensional vector, which is intended to indicate the full set of CFO resources. However, in practice, this product only allows for determining a single component of the CFO's resource vector. This is because the entirety of vector $w=(w_1,...,w_n)$ is effectively "spent" on this one component. There are no additional resources from the CSC that are "resource-equivalent" to this component within the EFC's resources.

This study presents a scheme of a positional differential game [Krasovskii N.N.], within which the problem under consideration is addressed. This means that the analysis is conducted from the perspective of the first player—the ally. Essentially, the CSC's resources have been directed towards additional funding for one specific EFC strategy. Consequently, the CSC lacks any remaining resources to support further allocations or funding of other EFC strategies.

In other words, all available CSC resources have been expended on a single EFC strategy. As a result, the EFC is in a position to continue its financing process using its remaining resources and strategies, thereby placing the CSC in a vulnerable position, as its resource (financial) capacity has already been depleted in support of only one of the multiple EFC strategies.

Therefore, it becomes necessary to divide the set of resources m into separate parts. This partitioning would enable the "equalization" of the efficiency of the EFC's resource sets across all components, matching them with proportional shares of the CSC's resources. To facilitate this, a set of elements within δ_j is introduced. This same approach can be applied to the set of EFC resources.

This study presents a framework of a positional differential game, within which the addressed problem is analyzed [13, 14]. This implies that the reasoning is conducted from the perspective of the first player—the ally. It assumes that no assumptions are made about the level of information available to the Education Financing Center (EFC), which is equivalent to a scenario where the EFC has full information. Consequently, the EFC can have a complete understanding of the state of the Cybersecurity Center (CSC) as well as all its actions and strategies.

At a given moment in time, the CKB, possessing resources $t \in [0,+\infty)$ $w(t) \in R_+^n$, transforms them into a new resource vector $Q \cdot w(t)$. Here, Q is the CKB's resource transformation matrix of order nnn, with all elements being positive. The elements q_{ij} of matrix Q are determined as follows. Let e_i $(i=1,...,n)$ denote one unit of the i-th RES of the first player. Then q_{ij}: $e_i = q_{ij} \cdot e_j$ $(j=1,...,n)$. In other words, q_{ij} indicates how much of the j-th RES of the first player is equivalent to one unit of the i-th RES of the first player. In financial and economic terms, this specifies the quantity of the j-th RES of the first player required to reproduce one unit of the i-th RES of the first player.

The CSC then makes a strategic move by choosing the quantity of resources $U(0) \cdot Q \cdot w(t)$, where $U(0)$ is a diagonal matrix composed of elements $u_i(t): 0 \leq u_i(t) \leq 1$. This magnitude of CSC resources leads to additional financing for the EFC, amounting to $\Xi \cdot S_1 \cdot U(0) \cdot Q \cdot w(t)$.

Similarly, the EFC, at time $t \in [0,+\infty)$ $g(t) \in R_+^m$, converts its resources into resources of size $H \cdot g(t)$. Here, H is the resource transformation matrix for the EFC, also of order m and consisting of positive elements. The elements h_{ij} of the matrix are H determined as follows. Let e_i $(i=1,...,m)$ denote one unit of the i-th RES of the second player. Then h_{ij}: $e_i = q_{ij} \cdot e_j$ $(j=1,...,m)$. In other words, h_{ij} indicates how much of the j-th RES of

the second player is equivalent to one unit of the i-th RES of the second player. In financial and economic terms, this represents the quantity of the j-th RES of the second player required to reproduce one unit of the i-th RES of the second player.

The EFC then makes its strategic move by choosing its resource amount $V(0)\cdot H\cdot g(t)$, where $V(0)$ is a diagonal matrix of order m, containing elements $v_i(t): 0 \le v_i(t) \le 1$. This magnitude of the EFC's resources also leads to additional financing for the EFC, amounting to $\Theta \cdot S_2 \cdot V(t)\cdot H\cdot g(t)$.

At time $t \in [0,+\infty)$, the resources of both players, the EFC and CSC, satisfy the following system of differential Eq. (1):

$$\begin{cases} dw(t)/dt = -w(t) + Q\cdot w(t) - U(t)\cdot Q\cdot w(t) - \Theta\cdot S_2\cdot V(t)\cdot H\cdot g(t) \\ dg(t)/dt = -g(t) + H\cdot g(t) - V(t)\cdot H\cdot g(t) - \Xi\cdot S_1\cdot U(t)\cdot Q\cdot w(t) \end{cases} \quad (1)$$

At the moment of time $t \in [0,+\infty)$ The following variants are possible:

$$(w(t), g(t)) \in G_2 \quad (2)$$

$$(w(t), g(t)) \in G_3 \quad (3)$$

$$(w(t), g(t)) \in G_4 \quad (4)$$

$$(w(t), g(t)) \in G_5 \quad (5)$$

where:

$$G_2 = \bigcup_{i=1}^{m} \{(w,g) : (w,g) \in R^{n+m}, w > 0, \quad g_i = 0\}$$

$$G_3 = \bigcup_{i=1}^{n} \{(w,g) : (w,g) \in R^{n+m}, \quad g > 0, w_i = 0\}$$

$$G_4 = \left\{\bigcup_{i=1}^{n} \left\{(w,g) : (w,g) \in R^{n+m}, w_i = 0\right\}\right\} \bigcap \left\{\bigcup_{i=1}^{m} \left\{(w,g) : (w,g) \in R^{n+m}, g_i = 0\right\}\right\}$$

$$G_5 = \operatorname{int} R_+^{n+m}.$$

Condition (2) indicates that the CSC has sufficient resources to interact with the EFC, while the EFC lacks resources. In this case, the interaction ends.

Condition (3) indicates a situation where the EFC has sufficient resources to interact with the CSC, while the CSC lacks resources. In such a case, the interaction also ceases.

Condition (4) states that both players do not have enough resources to continue the interaction, which also leads to its completion.

If Condition (5) is met, the interaction process between the players continues.

The financing process described in system (1) is considered within the framework of a positional differential game of quality with several terminal surfaces [16, 17]. We focus on analyzing the problem from the perspective of the first allied player, given the symmetry of the conditions. The problem, considered from the position of the second allied player, is solved in a similar way.

Let's denote by $T^* = [0, +\infty)$—time interval.

Definition. A pure strategy $U(.,.,.)$ for the first player (ally) is defined as a set of functions $u_i(.,.,.): T^* \times R_+^{n+m} \to [0,1], (i = 1,...,n)$, such that $u_i(t,(w,g) \in [0,1], (t \in T^*, (w,g) \in R_+^{n+m})$. Specifically, a pure strategy for the first player (ally) is a predetermined set of actions or decisions made to protect cybersecurity. The second player (opponent) then chooses their strategy $V(.)$ based on any information. For example, a pure strategy of the CSC (player-ally). Suppose the CSC decides to implement a comprehensive protection system that includes: a) Installing a modern firewall; b) Implementing a multi-factor authentication system; c) Implementing a SIEM. This is a specific set of actions that represents a pure strategy of the CSC. Then, the strategy of the EFC (player-opponent) is determined based on the fact that the EFC, knowing about the actions of the CSC, can choose its own strategy. For example, implement such strategies: a) increase funding for the implementation of a new online learning system; b) invest in cloud storage for educational materials; c) expand communication opportunities with students using social networks. Accordingly, the CSC seeks to determine such initial conditions (for example, the initial budget, the number of personnel, the current level of protection) under which it will be able to ensure the required level of cybersecurity, despite the actions of the EFC.

For example, the CSC might seek answers to questions such as: 1) With what minimum initial budget can we ensure protection from all major cyber threats? 2) What is the minimum number of cybersecurity specialists that the university initially needs to cope with the increased load due to new IT systems? 3) What level of basic protection should we have initially so that we can successfully resist new threats arising from the expansion of the university's digital infrastructure? In fact, the CSC seeks to find such initial conditions under which it can ensure the necessary level of cybersecurity, regardless of which strategy the EFC chooses to expand the use of IT in education. That is, the first allied player seeks to find a set of its initial states that have the following property.

Property: If the game starts from the initial states, the first allied player can choose a strategy $U_*(.)$ that ensures the fulfillment of Condition (2) at a specific point in time t. Moreover, this chosen strategy prevents the EFC from fulfilling Condition (3) at previous points in time. In other words, this property indicates that the first allied player can select a strategy guaranteeing that, at some moment in time t, the EFC will lack sufficient resources to fund its technological strategies further. Thus, the first allied

player's strategy should be such that it reduces the resource capabilities of the EFC to a level where additional financing of its technological strategies becomes impossible.

A set of such states represents the preferences of the first allied player, Y_1, whose strategies we will denote as $U_*(.)$'s strategies. The CSC, with its specified properties, represents $U_*(.)$'s optimal strategies.

The goal of the first allied player is to find preference sets. They also find strategies that, when applied, will lead to the fulfillment of Condition (2).

The described model is a bilinear differential quality game with multiple terminal surfaces [18].

The following paragraph presents the conditions that will allow us to find a solution to the game. That is, we can find 'preference' sets. Y_1 and optimal strategies $U_*(.)$ of the first player-ally (CSC).

B. Solution to Problem 1

A brief outline of the analytical solution to problem 1 is presented in this article for one of the variants of the game's parameter ratio. Solutions for other variants can be found similarly, utilizing the potential of cybernetic modeling tools.

Let us introduce the following notation: $B_1 = Q$, $B_2 = H$, $D_1 = \Xi \cdot S_1$, $D_2 = \Theta \cdot S_2$.

The solution to problem 1 depends on the ratio of parameters that determine the interaction between the first player-ally and the second player-opponent.

For all cases of the ratio of parameters, we will present in the form of two cases.

Case 1:

$D_1 \cdot B_1 \cdot D_2 \le B_2$, $B_2 \cdot D_1 \ge D_1 \cdot B_1$, $D_2 > 0$ (these are matrix inequalities),

$D_2 \cdot B_2 \cdot D_1$—Diagonal matrix;

$$[\{\{[\sum_{\theta=1}^{m}(D_2 \cdot B_2)_{i\theta} / (\sum_{j=1}^{m}(D_2 \cdot B_2)_{ij})] \cdot [(D_1 \cdot B_1)_{\theta 1} + ... + (D_1 \cdot B_1)_{\theta n}\} / [(D_2 \cdot B_2)_{i1} + ... + (D_2 \cdot B_2)_{\theta i}]\}^{0.5} \ge \max(\varphi_i, f_i) \quad (6)$$

$$\varphi_i = \max_j [(D_2 \cdot B_2)_{ij} / [\sum_{j=1}^{m}(D_2 \cdot B_2)_{ij}] / (D_2)_{ij}] \quad (7)$$

$$f_i = (D_2 \cdot B_2 \cdot D_1)_{ii} / [\sum_{j=1}^{m}(D_2 \cdot B_2)_{ij}] \quad (8)$$

Case 2:

When analyzing the interaction between the CSC and the EFC, several scenarios can be distinguished, depending on the ratio of their parameters and initial conditions.

Scenario 1: CSC Advantage. In this situation, the CSC can achieve its goal of ensuring the necessary level of cybersecurity due to favorable initial conditions. For example, the CSC may start with a significant advantage in resources, such as a substantial initial budget for cybersecurity, a team of highly qualified specialists, and access to advanced data protection technologies. At the same time, the EFC may face limitations that prevent it from fully realizing its goals for digitalizing education, such as limited funding for new IT systems or a lack of technical specialists to deploy new educational platforms.

Scenario 2: Equal Opportunities. In this scenario, both the CSC and the EFC start with comparable resources and capabilities. For example, both centers may have similar budgets, access to modern technologies in their respective fields, and teams with a comparable level of expertise. In such a situation, the success of each center will depend on their ability to effectively utilize available resources and adapt to the other's actions. The CSC can focus on developing flexible cybersecurity and data protection systems that can quickly respond to new threats arising from the EFC's IT innovations. In turn, the EFC can prioritize educational technologies that incorporate a high level of built-in security.

It should be noted that these scenarios are idealized cases, and the real situation may be somewhere in between them or have a more complex structure of interaction between the players.

Further, we introduce the following notations:

$$W_1 = \{(w(0), g(0)) : (w(0), g(0)) \in R_+^{n+m}, [(B_2^{i,\Sigma}) / (D_1 \cdot B_1)^{i,\Sigma}] \cdot [g(0)]_i < \sum_{j=1}^{n}(D_1 \cdot B_1\}_{ij} \cdot w_j(0), \exists i : i = 1,...,n;\} \quad (9)$$

$$W^* = \{(w(0), g(0)) : (w(0), g(0)) \in R_+^{n+m}, (q_*)_i \cdot (w(0))_i \ge [\sum_{\theta=1}^{n}(D_2 \cdot B_2)_{i\theta} \cdot (g(0))_\theta] / [\sum_{j=1}^{n}(D_2 \cdot B_2)_{ij}], \forall i = 1,...,n;\} \quad (10)$$

where:

$(q_*)_i = [D_2^{i,\Sigma} / D_1 \cdot B_1)^{i,\Sigma}]$,

$(B_2^{i,\Sigma})$ – sum of elements, i - The strings of the matrix B_2;

$(D_1 \cdot B_1)^{i,\Sigma}$ – sum of elements, i - The strings of the matrix $D_1 \cdot B_1$;

$Y_1 = W_1 \cap W_1^*$.

The outcome of the players' interaction is represented in a theorem that describes the preference set Y_Y of the first player (ally), which reflects the advantage of this player over the opponent. This advantage is expressed in the following ways:

The quantity of resources available.

The efficiency of resource allocation, represented in matrices S_1 and Ξ.

The implementation of the optimal strategy $U^*(.,.)$.

$$R_+^n \times R_+^m \mapsto R_+^n, U^*(w, g) = E \quad (11)$$

where: $E-$ is the identity matrix of order n, \times $(w, g) \in Y_1$ and is undefined otherwise.

It is important to note that the methodology for determining optimal strategies and preferred initial conditions is applicable to both the CSC and the EFC, despite their different roles in our model. For the CSC, the process of determining optimal strategies and the most

favorable initial conditions is based on the analysis of various scenarios for the development of the cybersecurity situation in the educational environment. In this case, the CSC assesses which initial resources and which strategic decisions will allow it to most effectively ensure cybersecurity and protect the information infrastructure of universities, taking into account the possible actions of the EFC to digitalize education.

For the EFC, a similar approach is used, as the EFC also conducts an analysis to determine its optimal strategies and preferred initial conditions. However, the focus here shifts to assessing which initial resources and which strategic decisions will allow for the most effective implementation of innovative educational technologies, taking into account the need to ensure their cybersecurity and the possible response actions of the CSC.

The pseudocode representing the key steps of your model is presented below:

Algorithm 1: Financing Game Model

Input:
w0—Initial resources of CSC (Cybersecurity Center),
g0—Initial resources of EFC (Education Financing Center),
Q—Transformation matrix for CSC,
H—Transformation matrix for EFC,
S1—Payoff matrix for EFC strategies,
S2—Payoff matrix for CSC strategies,
ξ—Resource allocation matrix for EFC,
θ—Resource allocation matrix for CSC,
Output:
Y—Preference set of CSC,
*U**—Optimal strategy for CSC,
*V**—Optimal strategy for EFC.

Steps:
1: Initialize transformation matrices *Q*, *H*, *S1*, *S2*, ξ, and θ.
2: Define differential equations for resource dynamics:
$d(w)/dt = -(Q \times U \times S1 \times \xi) + (g \times H \times V \times \theta)$
$d(g)/dt = -(H \times V \times S2 \times \theta) + (w \times Q \times U \times \xi)$
3: Identify preference set *Y* for *CSC*:
3.1: For each possible initial state (*w0*, *g0*):
Compute resource ratios (*p1*, *p2*) for each strategy.
Exclude strategies with inefficient resource allocations.
3.2: Add valid states (*w0*, *g0*) to the set *Y*.
4: Determine optimal strategies:
*U** ← Select CSC strategy minimizing EFC's ability to allocate resources.
*V** ← Select EFC strategy maximizing education quality improvement.
5: Conduct computational experiments:
5.1: For each state (*w0*, *g0*) in *Y*:
Simulate resource dynamics over time using the defined equations.
Analyze trajectories and equilibrium points.
5.2: Visualize preference set and balance rays.
6: Output results:
Return *Y*, *U**, and *V**.
Plot preference set and resource dynamics.

The main steps can be summarized as follows: Formulating the problem, i.e., defining two players (CSC and EFC), their strategies, and interdependencies. Constructing systems of differential equations to describe the interactions. Determining the set of preferences and optimal strategies.

Thus, although the goals of the CSC and the EFC are different, the methodological approach to determining their optimal strategies and preferred initial conditions is similar, which will allow for the analytical creation of a balanced model that takes into account the interests of both parties in the process of digital transformation of the higher education system of the Republic of Kazakhstan.

C. Constraints Adopted in the Game for the Given Problem Statement

1) Time-invariant system parameters

The current model assumes that parameters affecting the system remain constant throughout the analysis. This simplification has allowed us to focus on the interactions between players, but it limits the model's accuracy in a dynamically changing environment where time-varying factors can significantly influence outcomes.

2) The bilinearity of the system of differential equations

The proposed model is based on a bilinear structure, which implies linear dependencies between variables within certain limits. While this simplification makes the model more manageable, it may not fully reflect the complex nonlinear interactions that are often observed in real-world scenarios of university financing and informatization.

3) The nature of the problem statement

The formulation of the problem in the model is schematic, which has allowed us to highlight the key aspects of the interaction between the participants. However, this also leads to the neglect of some important factors, such as cultural, organizational, or technical features that can significantly influence the decision-making process.

Taking into account these limitations and their potential removal is an important direction for future research. In particular, in future works, we propose to consider the possibility of introducing time dynamics into the model, as well as studying the influence of nonlinear dependencies and taking into account more detailed aspects of the interaction between participants. This will allow us to increase the accuracy and applicability of the model in real-world conditions.

Let us note the following. The requirement of bilinearity should not be viewed as a serious limitation, since the strategies employed by the players may be nonlinear functions, which automatically renders the system under consideration nonlinear. When extending the model to scenarios involving more than two players, the next stage of research will consider interaction time frames ranging from one academic semester to three years. In our view, such a range will capture both short-term digitalization projects and long-term programs for modernizing IT infrastructure and ensuring cybersecurity in universities.

It should be noted that, when adapting the model for use with real-world data, it is essential to take into account the ethical and legal requirements of international standards. In particular, the collection and processing of information

on funding, IT infrastructure, and cybersecurity incidents must comply with the principles of FAIR Data, as well as personal data protection regulations (e.g., GDPR, ISO/IEC 27018). Furthermore, the methodology for data collection should undergo an internal approval process involving representatives of universities, government agencies, and independent experts. This will ensure transparency and reproducibility of results in practice.

V. Computational Experiment for Evaluating Player Resources in the Process of Improving Education Quality

A computational experiment was conducted to evaluate the resources of both players on a set of synthetic data, and the strategies described earlier were analyzed. The model was implemented in Python using the PyCharm development environment, and the results of the players' interaction are visualized in Fig. 1.

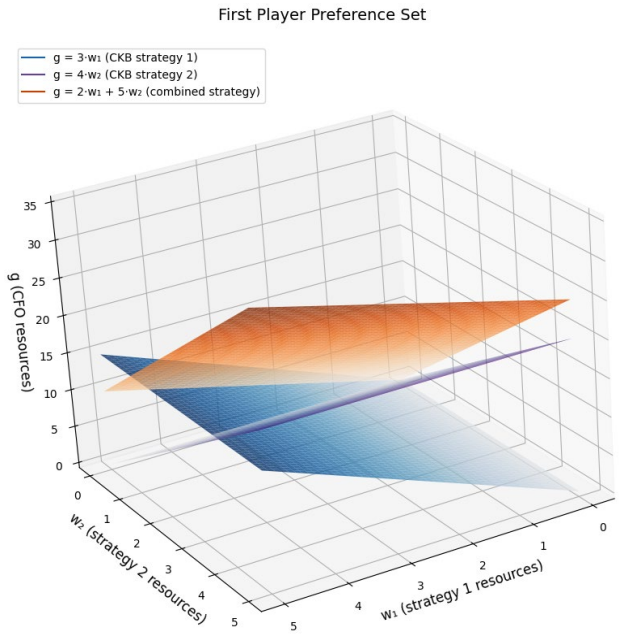

Fig. 1. Preference set of the first player-ally (University Cybersecurity Center).

The experiment plan included the following stages: 1) defining the initial positions of the players; 2) constructing, based on the proposed model, colored hyperplanes indicating the boundaries of the preference region of the first player-ally; 3) identifying the set of player states located below the hyperplanes in the positive orthant, indicating that when starting interaction from these points, the first player-ally can choose a strategy leading to the desired result; 4) determining the intersection of the hyperplanes and finding the balance ray, on which the states of both platforms are in equilibrium; 5) analyzing the resources of both players; 6) evaluating the effectiveness of achieving goals by both players with the chosen strategies and analyzing the trajectories of changes in their states relative to the balance ray. It should be noted that the ray of balance represents a set of initial states of the players, which, first, form a ray in the geometric sense, and second, for such initial states, there exist strategies that allow the players to remain on this ray for an arbitrarily long period of time.

The consideration of such an experimental setup enables the players, when addressing practical issues, to determine their strategies for allocating financial resources to achieve their objectives.

VI. Discussion of the Results of the Computational Experiment

The preference set of the first allied player is depicted in the positive orthant of a three-dimensional space. It represents a set of player states located "under" hyperplanes of different colors. The blue hyperplane $g = 3 \cdot w_1$ shows the ratio between the resources of the EFC and the first strategy of the CSC, while the pink hyperplane $g = 4 \cdot w_1$ reflects the ratio between the resources of the EFC and the second strategy of the CSC. The orange hyperplane $g = 2 \cdot w_1 + 5 \cdot w_2$ represents a combined strategy that takes into account both CSC strategies. The area beneath all three colored planes indicates states where the CSC has an advantage over the EFC. The intersection of the hyperplanes defines the boundaries of the preference region for the first allied player and allows for the determination of balance rays.

These balance rays have the following property: if the interaction between players begins from states along these rays, each player has strategies that enable them to remain on these rays for as long as desired. In this context, the CSC and EFC maintain a balance between cybersecurity and a sufficient level of education quality.

It should be noted that experiments conducted with different sets of initial data yield the same 'picture' of the process; therefore, their detailed description has been omitted. The application of the proposed approach in universities of the Republic of Kazakhstan has confirmed its high effectiveness.

This study is theoretical in nature and does not utilize data from individuals or specific institutions. All computational experiments were conducted using synthetic data for methodological demonstration purposes.

Although synthetic data were employed, the model's structure and computational algorithms were designed in such a way that they can be directly adapted to empirical datasets. For instance, the parameters of the matrices may be independently specified by universities on the basis of institutional statistics regarding budget allocation, cyber threat indicators, and the quality of educational services. This design enables subsequent cross-validation of the simulation outcomes against real-world cybersecurity scenarios. Furthermore, it allows for comparative assessment of the simulation results with alternative approaches to resource allocation for security provision, where necessary.

As an intermediate step toward empirical validation, a series of supplementary model scenarios was conducted. These scenarios incorporated parameters that approximate the operational conditions of universities in Kazakhstan and Ukraine. The detailed results of these tests are

intended to be presented in a separate publication devoted to the practical implementation and validation of the proposed model.

VII. Conclusion

In the course of the research, a game-theoretic model for financing the informatization of education was developed, taking into account aspects of computer security, with a focus on the financial interaction between players. The novelty of the model lies in the use of a differential quality game with a bilinear structure, where the financial states of the players are described by a system of differential equations. In this formulation, the model allows for the determination of preference sets and optimal strategies for players, which was demonstrated in a computational experiment. The conducted analysis confirms that the proposed model effectively evaluates strategic interactions between participants, ensuring consideration of cybersecurity. Visualization of the preference set for the first player, the CSC, demonstrates the applicability of the model for solving practical problems of financing the informatization of the educational process. In the future, it is possible to expand the model to integrate real data and more complex strategic scenarios.

As a priority direction for future research, an empirical validation of the model is planned using data from Kazakhstani universities in collaboration with universities in Ukraine, Azerbaijan, and Kyrgyzstan. To this end, additional partnerships will be established with a number of higher education institutions in the Republic of Kazakhstan and Ukraine, within which supplementary anonymized statistical data will be collected on IT project funding volumes, cybersecurity levels, frequency of cyber incidents, and indicators of educational service quality. Comparing the model's results with actual data will make it possible, in the next stage of research, to validate its predictive accuracy and identify parameters that require adjustment in order to enhance its practical applicability.

Statement on the Use of Generative AI and AI-Based Technologies in the Writing of this Article

This study is theoretical in nature. It does not involve experiments with human or animal participants; therefore, no formal approval from institutional management was required. The data used in this work do not contain any personal information. Generative artificial intelligence tools were not employed in the creation or modification of research data, mathematical models, or the original experimental results. The use of AI-assisted tools during the writing process was limited to editorial support and did not affect the scientific content of the study.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, Arkadii Chikrii, Valery Lakhno, Volodimir Malyukov; methodology, Arkadii Chikrii, Valery Lakhno, Volodimir Malyukov; software, Inna Malyukova, Berik Akhmetov; validation, Kaiyrbek Makulov, Bagdat Yagaliyeva; formal analysis, Inna Malyukova, Berik Akhmetov; investigation, Valery Lakhno, Volodimir Malyukov; resources, Kaiyrbek Makulov, Bagdat Yagaliyeva; writing—original draft preparation, Valery Lakhno, Volodimir Malyukov, Bagdat Yagaliyeva; writing—review and editing, Valery Lakhno, Volodimir Malyukov; funding acquisition, Kaiyrbek Makulov, Bagdat Yagaliyeva. All authors had approved the final version.

References

[1] S. AlDaajeh *et al*., "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput. Secur*., vol. 119, 102754, 2022.

[2] M. Lehto, "Cyber security education and research in the Finland's universities and universities of applied sciences," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global*, 2018, pp. 248–267.

[3] T. A. A. Alhumud, A. Omar, and W. M. Altohami, "An assessment of cybersecurity performance in the Saudi universities: A total quality management approach," *Cogent. Educ*., vol. 10, no. 2, 2023.

[4] A. M. Elsawy and O. Ahmed, "E-Learning using the blackboard system in light of the quality of education and cyber security," *International Journal of Current Engineering and Technology*, vol. 9, no. 1, pp. 49–54, 2019.

[5] T. H. Selim, "The education market in Egypt: A game theory approach," in *Proc. Economic Research Forum Annual Conference*, 2007.

[6] G. N. Beltadze, "Game theory-basis of higher education and teaching organization," *Int. J. Mod. Educ. Comput. Sci*., vol. 8, no. 6, 2016.

[7] Y. Ekinci, B. Z. Orbay, and M. A. Karadayi, "An MCDM-based game-theoretic approach for strategy selection in higher education," *Socioecon. Plann. Sci*., vol. 81, 101186, 2022.

[8] H. Correa and G. W. Gruver, "Teacher-student interaction: A game theoretic extension of the economic theory of education," *Math. Soc. Sci*., vol. 13, no. 1, pp. 19–47, 1987.

[9] O. Jadreskic, L. Cerovic, and A. Segota, "Game theory and its application in analysis of relationship between educational system and Labour Market," in *Proc. 18th International Scientific Conference on Economic and Social Development*, 2016.

[10] C. Liu, H. Wang, and Y. Dai, "Sustainable cooperation between schools, enterprises, and government: An evolutionary game theory analysis," *Sustainability*, vol. 15, no. 18, 13997, 2023.

[11] K. Makulov *et al*., "Cloud platform selection model in the framework of differential quality game with fuzzy information," *IEEE Access*, vol. 13, pp. 22578–22589, 2025.

[12] A. A. Chikrii, *Conflict Controlled Processes*, Netherlands: Springer Science & Business Media, 2013.

[13] A. I. Zourmpakis, M. Kalogiannakis, and S. Papadakis, "Adaptive gamification in science education: An analysis of the impact of implementation and adapted game elements on students' motivation," *Computers*, vol. 12, no. 7, 143, 2023.

[14] H. M. Selim, "Critical success factors for e-learning acceptance: Confirmatory factor models," *Comput. Educ*., vol. 49, no. 2, pp. 396–413, 2007.

[15] H. Correa and G. W. Gruver, "Teacher-student interaction: A game theoretic extension of the economic theory of education," *Math. Soc. Sci*., vol. 13, no. 1, pp. 19–47, 1987.

[16] A. Parrish *et al*., "Global perspectives on cybersecurity education for 2030: A case for a meta-discipline," in *Proc. Companion 23rd Annu. ACM Conf. Innov. Technol. Comput. Sci. Educ*., 2018, pp. 36–54.

[17] O. Y. Burov *et al*., "Cybersecurity and innovative digital educational environment," *Inf. Technol. Learn. Tools*, vol. 6, no. 80, pp. 414–430, 2020.

[18] S. Yusif and A. Hafeez-Baig, "Cybersecurity policy compliance in higher education: a theoretical framework," *J. Appl. Secur. Res*., vol. 18, no. 2, pp. 267–288, 2023.

[19] A. Piazza, S. Vasudevan, and M. Carr, "Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector," *J. Cybersecurity*, vol. 9, no. 1, 2023.
[20] T. Crick, J. H. Davenport, A. Irons, and T. Prickett, "A UK case study on cybersecurity education and accreditation," in *Proc. 2019 IEEE Frontiers Educ. Conf. (FIE)*, 2019, pp. 1–9.
[21] P. Benlloch-Caballero, Q. Wang, and J. M. A. Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," *Comput. Netw*., vol. 222, 109526, 2023.
[22] B. Tang *et al*., "Time-delay signature concealment in a security-enhanced optical system with dual-loop electro-optic self-feedback phase encryption," *IEEE Photonics J*., vol. 15, no. 1, pp. 1–8, 2023.
[23] N. Dragicevic, A. Ullrich, E. Tsui, and N. Gronau, "A conceptual model of knowledge dynamics in the industry 4.0 smart grid scenario," *Knowl. Manag. Res. Pract*., vol. 18, no. 2, pp. 199–213, 2020.
[24] C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, Eds., *Game Theory and Machine Learning for Cyber Security*, Hoboken, NJ, USA: Wiley, 2021.
[25] I. Kalderemidis *et al*., "GTM: Game theoretic methodology for optimal cybersecurity defending strategies and investments," in *Proc. 17th Int. Conf. Availability, Rel. Secur*., 2022, pp. 1–9.
[26] M. Pujari, A. K. Pakina, and A. Sharma, "Enhancing cybersecurity in edge AI systems: A game-theoretic approach to threat detection and mitigation," *IOSR J. Comput. Eng*., vol. 25, no. 3, pp. 65–73, 2023.