UDC 004.056

*V.A. Lakhno (professor, National University of Life and Environmental Sciences of Ukraine, Ukraine)*
*B.S. Akhmetov (director of the Center for advanced studies and distance education, Kazakh National Pedagogical University named after Abay, Kazakhstan)*
*L.M. Kydyralina (doctoral, Kazakh National Pedagogical University named after Abay, Kazakhstan)*

# Decision support on mutual investment in cybersecurity of the information and educational environment of the university

*There was considered the problematic of search for rational variants of mutual investment control strategies in the systems of cyber security of large educational institutions, for example, universities of Kazakhstan and Ukraine. Was announced the model intended as an information and algorithmic component for the decision support system designed by us in the tasks of analyzing and optimizing mutual investment strategies in the information and educational environment of educational institutions and their cybersecurity systems. Our solution, unlike the works of other authors in this segment of scientific research, differs in the ability to determine specific parameters and recommendations in the process of mutual investment. The model and the software product create prerequisites for optimizing management decisions in the investment process to the information and educational platforms and to the cybersecurity of educational institutions.*

The modern information and educational environment based on innovative globalized educational programs is often realized by integrating educational institutions with leading research and production enterprises or with foreign educational institutions (EI). International investment projects in the field of education and, in particular, in digital information and educational platforms, have become a common practice of international cooperation [1, 2]. Such investment projects, in our opinion, must necessarily assume a deep analysis of financial strategies for ensuring the cybersecurity of the EI and their joint information and educational environment. As many experts on information protection (IP) note the cybersecurity systems (CSS) of EI, in particular, large international, state and private universities, should not only ensure the security of information arrays and data, including confidential ones, but also guarantee the impossibility of external unauthorized invasion to the information and educational environment (IEE) of these EI [2, 3]. The constant growth of the cybercrime in the world only increases the need to enlarge financial investments in the CSS [4-6], in particular for the EI.

We should note that to the protected information that is stored and circulated in the EI there can be attributed [2, 4, 7]: personal data of students, teachers, employees; digitized information representing the intellectual property of the educational institution; information arrays that provide the learning process (for example, multimedia content, databases, training programs, innovative software); etc. This information can act as an object of theft or distortion from external (internal) computer intruders (CI) or from hooligan motives, from students or employees.

In many EI (in particular schools, colleges, universities, student campuses, etc.) there is preserved the traditional approach for solving the problems of financing the means and systems of information protection (IP) and cybersecurity (CS) [1, 2]. Most of the financing strategies in the CSS involve only allocating funds for antivirus programs and relatively simple network protection tools [2, 3]. This is a very simple financial strategy for cyber protection of EI. Even experienced administrators of information and cybersecurity services are not always ready for the worst case scenario for cyberattacks against computer systems and EI networks [2, 3]. The information protection side needs to shift its focus to changing the traditional approaches of CSS financing. For example, changing the financial component of CS investment strategies to a policy that involves the detection and blocking of potential hacking of computer systems and EI networks [4].

The procedure of innovative projects investment, in particular in the area of the digital education technologies development with the emphasis on the formation of the information and educational environment (IEE) of EI, is often characterized by a high degree of uncertainty and riskiness in the tasks of ensuring the EI cybersecurity. The landscape of cyberthreats, that has changed in recent years [5, 6], had a fundamental influence on the attitude to the CS problems of many EI [1, 2]. First of all, it was due to the significant potential vulnerabilities and cyberthreats for IEE of EI, to the occurrence of new classes of cyberattacks, to the widespread use of wireless data transmission technologies, etc. In conditions of rapid implementation of digital technologies in education, not all investors, for example, creating private and, including large international universities in Jordan, Ukraine, Kazakhstan, paid due attention to the problem of IEE cybersecurity (CS) of EI [1, 2, 5]. We also note that not many publications in this area contain descriptions of models related to the finding of different strategies for the mutual financial investment of the EI in the CSS [3, 4].

In order to improve the effectiveness of evaluating various investment projects in CSS of EI, and subsequent decision-making related to investing, it is necessary to use modern information technologies [5], for example, technologies that are based on the application of decision support systems (DSS) [6, 7].

The filling of the informational-algorithmic component of the DSS can be realized by the implementation of blocks that contain algorithms for economic and mathematical models for investing in the in CSS of EI.

In connection with the foregoing, it is urgent to develop new economic and mathematical models for DSS that will adequately describe the actual processes of CSS financing. This will make it possible rationally to choose the financing strategies for the CSS of EI.

A large number of publications have been devoted to the researches of the effective strategies for financial investment in CSS, in particular for EI, [4-7]. The development of computer systems and information technologies gave a rise to a separate concept of work on CSS investment optimization. This concept of research is based on the extensive use of expert systems (ES) [7-9] and DSS [10-12] in the tasks of determining rational investment strategies in the field of CS. We have studied quite a lot of works in this area and have come to the conclusion that most of these publications do not contain concrete decisions on the choice of rational strategies for mutual financial investment in CSS of EI. Also, as follows from the conclusions of [8, 9, [11, 12], the use of ES and DSS in order to automate procedures for selecting rational investment control strategies in CSS is not always accompanied by clear recommendations.

These circumstances caused the problem associated with the need to develop new models for DSS in the tasks of determining rational strategies for mutual financial investment in CSS of EI.

On the basis of the previous experience and approaches, described by the authors in earlier publications on this subject [8, 9, 11, 12], and also works close to the methodology of research by the external authors [1, 4, 6, 7, 13-18], we can prove that a fairly effective approach for solving this class of problems is the use of methods of the differential quality games theory with several terminal surfaces [11, 19].

**Therefore, the analysis of publications on this topic confirmed the relevance of the problem of further development of models for DSS in the tasks of continuous mutual investment in CSS of EI. The last one is especially important for cases when it is necessary to develop clear recommendations for investors. But there is no need to apply complex mathematical calculations, because most of the calculations are performed by computer programs.**

**In our researches [11, 20] there are described the models for searching rational variants of investment control strategies in cybersecurity systems (CSS) of educational institutions and relevant information and educational platforms. The model is an information component for the developed decision support system in the tasks of analyzing various investment strategies in CSS of educational institutions, primarily, of large international universities that seek to provide reliable cyberprotection for their information and educational platforms and their content.**

## References

1. Rezgui, Yacine, and Adam Marks. (2010). "Information security awareness in higher education: An exploratory study." Computers & Security 27.7 (2008): pp. 241–253.

2. Sultan, Nabil. "Cloud computing for education: A new dawn?." International Journal of Information Management 30.2, pp. 109–116.

3. Schneider, Fred B. (2013). "Cybersecurity education in universities." IEEE Security & Privacy 11.4, pp. 3–4.

4. Conklin, Art. "Cyber defense competitions and information security education: An active learning solution for a capstone course." The System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. Vol. 9. IEEE, 2006.

5. Schuett, Maria, and M. Rahman. (2011). "Information Security Synthesis in Online Universities." The arXiv preprint arXiv:1111.1771.

6. Gordon, L. A., Loeb, M. P., Zhou, L. (2016). Investing in Cybersecurity: Insights from The Gordon-Loeb Model, Journal of Information Security, 7(02), the PP. 49. DOI: 10.4236/jis.2016.72004.

7. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, 1(1), pp. 13–19.

8. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1(2(85)), pp. 4–15.

9. Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskii, V., Pupchenko, O. (2017). Development of the intelligent decision-making support system to manage cyber protection at the object of informatization, Eastern-European Journal of Enterprise Technologies, 2/9 (86), pp. 53–61.

10. Mariusz, N., Benton, M. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management [El. resource] Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf

11. Lakhno V., Malyukov V., Gerasymchuk N. et al. (2017). Development of the decision making support system to control a procedure of financial investment, Eastern-European Journal of Enterprise Technologies. Vol. 6, No. 3. pp. 24–41.

12. Akhmetov B. et al. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies. No. 1 (2). pp. 4–15.

13. Jalali, M., Siegel, M., Madnick, S. (2017). Decision Making and biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment [Electronic resource] Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.01031.pdf.

14. Radziwill, N., Benton, M. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management [Electronic resource] Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf

15. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: a real options perspective. Journal of Accounting and Public Policy, 34(5), 509-519.

16. Fielder, A., Konig, S., Panaousis, E., Schauer, S., & Rass, S. (2017). Uncertainty in Cyber Security Investments. arXiv preprint arXiv:1712.05893.

17. Cavusoglu H., Mishra B., Raghunathan S. A model for evaluating IT security investments, Communications of the ACM, 2004, Vol. 47, No. 7, 87–92.

18. Fielder A., Panaousis E., Malacaria P. et al. Decision support approaches for cyber security investment, Decision Support Systems, 2016, Vol. 86, 13–23.

19. Isaacs, R. (1999). Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization. Courier Corporation.

20. Berik Akhmetov, Valeriy Lakhno, Bakhytzhan Akhmetov, Yuri Myakuhin, Asselkhan Adranova, Lazat Kydyralina. Models and algorithms of vector optimization in selecting security measures for higher education institution's information learning environment // Lecture Notes in Artificial Intelligence, Springer, 2018, september, Prague. (In the press)