provide backup and recovery of information in case of loss. This is achieved by encrypting, archiving and authenticating data and ensures full management and access to confidential information from anywhere in the country at any time.

References:

1. Letychevskyi O.O. Suchasni naukovi problemy kiberbezpeky. *Visnyk NAN Ukrainy*. 2023. № 2. S. 12–20. URL: https://doi.org/10.15407/visn2023.02.012

2. Onyshchenko S., & Hlushko A. Analitychnyi vymir kiberbezpeky Ukrainy v umovakh zrostannia vyklykiv ta zagroz. *Ekonomika i region.* 2022. Vol. 1. Issue. 84. S. 13–20. URL: https://doi.org/https://doi.org/10.26906/EiR.2022.1(84).2540.

3. Levkin A., Levkina R., Petrenko A., & Chaliy I. Economic Security as a Result of Modern Biotechnology Implementation. *Problems of Infocommunications Science and Technology (PIC S T '2019): 2019 IEEE International Scientific-Practical Conference (Kyiv 8-11 October 2019).* Kyiv, 2019. Pp. 139–142.

UDC 04.002.658.5

D. Levkin, Candidate of Engineering Science, Assoc. Prof. (*SBTU, Kharkiv*)
O. Zhernovnykova, Dr of Pedagogical Science, Prof. *(H.S. Skovoroda KNPU, Kharkiv)*
Ya. Kotko, Candidate of Economic Sciences (*SBTU, Kharkiv*)

MODERN MATHEMATICAL METHODS IN THE CYBER SECURITY SYSTEM

A modern cyber security system ensures data processing and storage, confidentiality, availability and integrity of information. Various relationships between data types and methods of combating possible cyber attacks are based on known mathematical models and algorithms from computational methods for their implementation. Mathematical methods and computational methods are the basis of confidential information protection systems, detection and prevention systems of potential cyber threats. To increase the effectiveness of cyber protection of the data environment, it is necessary, if possible, to develop new mathematical models and methods of their implementation, as well as to modernize already existing mathematical models and computational methods that will take into account the specific features of the simulated systems [1, S. 6–13]. This, in turn, will complicate the type of boundary value problems, systems

of constraints on process control parameters, and computational methods for calculating the objective function.

Let's consider the most common methods used in the information cyber security system: signature methods highlight intrusions into the system and are used to protect the system from hacker attacks (constant introduction of a threat fragment and quick detection of threats using intelligent algorithms); mathematical models in the form of graphs are used to audit networks, to identify weak points in the cyber protection system and to analyze the correlations of cyber attack warnings; statistical methods are used to detect deviations or anomalies and form a profile of system behavior (for each element of the system, a certain number of probable values and confidence intervals of their deviations are formed); the method of element clustering is used to detect unknown attacks in the network, this method performs an analysis of selected data containing information about single objects with their subsequent ordering (a set of elements is divided into appropriate clusters and the degree of deviation from these clusters is revealed); the adaptive regression method models the relationship and interaction between variables (building an optimal approximating network using a set of vectors with variable vertices); support vector methods are used for classification and regression analysis [2, S. 133–144]. Note that when constructing mathematical models, an important stage is the determination of conditions that will guarantee the existence of a single solution of boundary value problems. The most urgent question is the correctness of boundary value problems when the object of research is a material of non-standard shape and internal structure under the influence of load sources. Thus, when performing mathematical modeling of a multilayer material under the action of sources of thermal load, the state of the modeled system is recorded using boundary value problems for nonlinear, inhomogeneous, multidimensional differential equations of thermal conductivity with the boundary conditions of the beginning and end of the thermal action and the boundary conditions of the specific heat flow. Due to the fact that, using the traditional theory of the existence and unity of the solution of boundary value problems, it is not possible to guarantee their correctness, the author suggests using the theory of pseudo-differential operators in the space of generalized functions. Having found the solution of the inhomogeneous boundary value problem, the conditions for the uniform boundedness of the fundamental function of the solutions of the homogeneous boundary value problem are determined. Using the parametric method, it is proved that the Fourier symbol of the basic differential equation of a nonhomogeneous boundary value problem consists of the sum of two symbols for which the conditions of uniform

limitation in the space of generalized functions of power growth (decrease) are fulfilled. obtained results [3, Pp. 91–102] make it possible to guarantee the correctness of the specified boundary value problems for systems of differential equations of thermal conductivity. We note that the correctness of boundary value problems determines the correctness of applied optimization mathematical models and the main task of detecting and controlling cyber threats in the information environment, which increases the quality of the functioning of the cyber information protection system.

The peculiarity of the above studies is their universality for increasing the effectiveness of controlling possible cyberattacks on information systems. According to the authors of the research, the given results, after their finalization, should be applied to increase the effectiveness of detecting potential cyberattacks on systems, to prevent network intrusions by minimizing existing cyber-defense deficiencies. This will allow more effective prevention of intrusion into the system and reduce the probability of leakage of confidential information due to the effective interaction of all system elements, their adaptability and high stability of the data network.

References:

1. Khlaponin Y.I., Kondakova S.V., Shabala Y.Y., Yurchuk I.P., & Demianchuk P.S. Analiz stanu kiberbezpeky v providnykh krainakh svitu. *Kiberbezpeka: osvita, nauka, tekhnika*. 2019. Vol. 4. Issue. 4. S. 6–13. URL: https://doi.org/10.28925/2663-4023.2019.4.613

2. Shevchenko S., Zhdanova Y., Skladannyi P., & Spasiteleva S. Matematychni metody v kiberbezpetsi: grafy ta yikh zastosuvannia v informatsiinii ta kibernetychnii bezpetsi. *Kiberbezpeka: osvita, nauka, tekhnika*. 2021. Vol. 1. Issue. 13. S. 133–144. URL: https://doi.org/10.28925/2663-4023.2021.13.133144

3. Levkin A., Abuselidze G., Berezhna N., Levkin D., Volkova T., & Kotko Y. The Quality Function in Determining the Effectiveness of Example Bioeconomics Tasks. *Rural Sustainability Research*. 2022. Vol. 48. Issue. 343. Pp. 91–102. DOI 10.2478/plua-2022-0019