UDC 623.618.51

Herasimov S., Shmatko O.

AUTOMATED DECISION-MAKING SYSTEM FOR MANAGEMENT OF INFORMATION PROTECTION CHANNELS

Decision-making tasks when managing information security channels are not automated at a sufficient level [1, 2]. This leads to the fact that decisions to block information transmission channels are made on the basis of subjective assessments of decision makers (DMs), or using insufficiently complete information models. At the same time, in the process of functioning of information transmission channels, the results of the work of bodies identifying and blocking information leakage channels are poorly taken into account [3, 4].

Thus, managing information security channels now actually means collecting and displaying information about a possible data leak. Then influence (blocking) is assigned to each information channel separately and is carried out, in fact, manually.

The purpose of this research is to develop a method for synthesizing an automated decision-making system for managing information security channels, which takes into account uncertainty in determining information leakage channels and allows us to ensure the required level of security [5, 6].

A feature of the proposed structural diagram is that it takes into account both intellectual and technical features when making decisions when managing information security channels. Note that by intellectual features we mean the conclusions and proposals of the decision maker for managing information security channels. It is proposed to include technical features for monitoring information transmission channels and technical means for identifying (blocking) channels of possible information leakage. The proposed structure simplifies further solution of research problems.

The solution to the problem of assigning impacts when managing information security channels to cover information leakage is to determine the possibility of redirecting information through other channels. This decision depends on the method of identifying the channel of information leakage (technical channels of information leakage), the means of information leakage (technical means of espionage), the software speed of information transmission, and the information dissemination program. When solving such a problem, the time required to determine the threat and methods of influence to eliminate it is also calculated [7].

Thus, when assigning impacts on information leakage channels and areas of possible information attacks, this is a difficult logical and analytical task to solve.

The final results of solving the problem of assigning impacts to block information leakage channels are assessed qualitatively - if possible, automated control of information security channels [5].

A structural diagram of information exchange in managing information security channels has been developed. This block diagram allows you to schematically represent the order of tasks to be solved in a synthesized automated decision-making system when managing information security channels to formalize decision-making tasks. A feature of the proposed structural diagram is that it takes into account both intellectual and technical results of decision-making when managing information security channels. The implementation of the proposed scheme allows us to take into account the influence of the decision maker (a priori data) and the characteristics of technical means of monitoring information transmission channels (a posteriori data).

A comparative assessment of strategies for the planned information security process involves solving a multicriteria optimization problem. The logical-linguistic production hierarchical model is justified as a mathematical model for determining protection parameters.

The main form of recording in it is interconnected tables of linguistic rules, which are a display connecting the previous, current and future states of the described process.

The process of determining information security parameters directly in the logical-linguistic hierarchical production model is difficult to trace. Therefore, this process is described using an algebraic model that is closest to a linguistic description. If it is inappropriate to synthesize products in order to reduce the number of production rules, it is proposed to use the fuzzy identification method. The method of formalizing knowledge to determine appropriate strategies for the planned information security process has been improved. It differs from the known ones in the formation of a set of production rules taking into account parameters that, when developing recommendations under conditions of non-stochastic uncertainty, describe a fuzzy environment. The method of processing knowledge to determine appropriate strategies for the planned information security process has also been improved. It differs from the known ones in the processing of knowledge based on the developed procedure for their algebraic approximation and fuzzy identification.

The development of this research consists in substantiating a multicriteria optimization problem in a fuzzy formulation when managing information security channels. Solving this problem will make it possible to determine a rational strategy for the planned information security process using an automated decision-making system.

References

1. O. Shmatko, S. Herasymov, Y. Lysetskyi and etc. **Development of the automated decision-making system synthesis method in the management of information security channels**, *Eastern-European Journal of Enterprise Technologies*, 2023, 6(9) (126), p.p. 39-49, https://doi.org/10.15587/1729-4061.2023.293511.

2. S. Yevseiev, V. Ponomarenko, O. Laptiev and etc. **Synergy of building cybersecurity systems: monograph**, Kharkiv: PC TECHNOLOGY CENTER, 2021, 188 p., https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=4700333.

3. S. Herasymov, V. Olenchenko, S. Yevseiev and etc. **Investigation of the Dynamic Filters' Characteristics for the Analysis of Random Signals During Data Transmission**, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), p.p. 162-166.

4. S. Herasimov, V. Soroka, S. Yevseiev and etc. **Development of a Method for Measuring small Nonlinear Distortions of Periodic Electrical Signals**, *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies* (ISMSIT), 2022, p.p. 49-52, https://doi.org/10.1109/ISMSIT56059.2022.9932685.

5. S. Herasimov, E. Roshchupkin. **Parameters of monitoring the technical condition of airspace radio engineering monitoring systems**, *International scientific and practical conference –Application of information technologies in the preparation and operation of law enforcement forces"*, March 15, 2022, p.p. 31-32.

6. S. Yevseiev, R. Hryshchuk, K. Molodetska and etc. **Modeling of security systems for critical infrastructure facilities**, Kharkiv: PC TECHNOLOGY CENTER, 2022, 196 p., https://doi.org/10.15587/978-617-7319-57-2.

7. S. Herasymov, A. Tkachov, S. Bazarnyi. **Complex Method of Determining the Location of Social Network Agents in the Interests of Information Operations**, *Advanced Information Systems*, 8 (1), p.p. 31-36, https://doi.org/10.20998/2522-9052.2024.1.04.