Cybersecurity Graph Model of Information Resources

Get access

Alexander V. Nesterenko
State Enterprise "Ukrainian Scientific Center for Development of Information Technologies", Kiev
Igor E. Netesin
State Enterprise "Ukrainian Scientific Center for Development of Information Technologies", Kiev

Краткое описание

With the growing activity of cyberattacks on automated information systems, the task of determining the priority of building protective equipment is becoming increasingly relevant. The model for solving this problem, based on the ontological description and graph representation of the system security environment, is proposed. The ontologies of threats, resources (objects), and protection mechanisms are developed. The proposed approach is based on construction and partitioning of the graph of the relations of threats and system objects into subgraphs (subsystems) as connected components of the original graph with subsequent finding the relative risks of the damage of these subsystems within the overall system to find out the subsystems to which should be given priority to increasing their security level. The risk assessments of resource damage are determined based on expert threat scores and expert scores of the level of harm (loss) from damage. The algorithm has been developed by which the relative risks of subsystems are calculated. Analytical expressions are given and the example is used to calculate the risks of damage of the objects for the system without the partition into subsystems and taking into account the partition, to detect critical subsystems for protection. Application of the model gives a clearer picture of the interaction of threats and system resources, helps one to find the most significant vulnerabilities of the system and to look for ways to improve its security in the process of solving practical tasks to ensure cybersecurity. The performed calculations confirm the correctness and adequacy of the proposed model, its simplicity and ease of use, providing an effective tool for experts and developers of security systems for automated information systems.
Ключевые слова: cybersecurity, information resources, threat, risk, ontology, graph model

ЛИТЕРАТУРА
ЦИТИРОВАНО В