ABSTRACT

Master's Thesis: __ pages, __ figures, __ tables, __ sources.

Comparative analysis of different approaches to the development of intrusion detection system as part of the proposed system for modelling network infection and countering the infection process.

The purpose of the proposed system is to simulate real threats to the security of the computer network and to create a system to counter these threats.

The subject of the study is the construction of a theoretical-game model of counteracting the system of intrusion detection of the process of attack on the network.

The object of the study is to create an intrusion detection system based on normal and abnormal network data.

The intrusion detection system has been learning in the normal operation of the network for some time, forming several clusters of data that characterize the normal operation of a properly configured network. To detect threats, the trained system checks how close the current data is to one of the clusters, which reveals anomalies in the deviation of the values of the new measurements from the average relative to the data on which it was trained.

The simulation system considers the interaction of the attacker and the anomaly detection system from the standpoint of game theory, where the attacker and the system build their strategy with respect to the information they know. The implementation of this simulation system was implemented and tested on an open set of real data on a computer network. The GNG algorithm performed much better than IGNG in the implementation presented. The effectiveness of clustering by the intrusion detection system is almost independent of the number of parameters observed. The speed and quality of the attacker simulation system and the intrusion detection system are satisfactory.

Further research may include the use of more sophisticated clustering algorithms, the implementation of multithreading into an intrusion detection system, the use of honeypot data in training the detection system, and the optimization of the modeling system by adding reflection to the model at run time.

CYBER SECURITY, CYBER THREATS, MULTI-AGENT SYSTEMS, INTERVENTION DETECTION SYSTEMS, MODELING SYSTEM, NEURAL GAS, CLUSTERIZATION