MODERN METHODS OF COUNTERING ATTACKS ON WIRELESS NETWORKS

Zamiesov K. S., Kramskyi A. A., Zaporozhets I. V.
National Technical University «Kharkiv Polytechnic Institute», Kharkiv

In today's digital environment, information security is becoming increasingly important, as the number and complexity of cyber threats are growing rapidly. Countering cyberattacks is one of the main ways to protect the network resource of information computer systems. Despite the fact that these systems have been in use for several decades, many highly qualified specialists are engaged in their development, and a large number of articles have been devoted to the creation of the corresponding scientific and methodological base, practical experience shows that measures to counteract network cyberattacks suffer from a number of significant shortcomings. The most important of them is the inaccuracy in recognizing the full scale of cyberattacks on networks, which is confirmed by known cases of successful hacking of computer security systems in many countries. In addition, incorporating known tools to counter network cyberattacks into national information security systems requires complex adaptation to different contexts of use. Artificial intelligence-based attacks that use powerful machine learning algorithms, neural networks and other advanced techniques to bypass traditional defenses pose a particular challenge. These attacks are becoming increasingly sophisticated and adaptive, making it harder to defend computer systems. Research shows that recognizing cyber attacks on networks relies on the use of artificial neural networks. This is due to the fact that leading cybersecurity vendors (Cisco and Symantec) have proven their ability to improve the effectiveness of using ANNs for such tasks, and have also proven the ability of neural network tools to adapt to different use cases. Methodological and theoretical basis for effective implementation of neural networks in SPAs is provided by theoretical developments and experience in creating computer security systems by Ukrainian and foreign scientists.

The development of effective neural models and methods for countering cyberattacks that adapt to operating conditions and ways to quickly respond to new types of cyberattacks is the main stage of our work to achieve this:

- analyze the capabilities of neural network means of countering cyberattacks on the network resources of information systems;
- to build a conceptual model of ensuring the effectiveness of neural network counteraction to cyberattacks;
- develop a model for the formation of parameters of initial examples;
- to develop a neural network model for countering cyberattacks using expert knowledge.

One of the main ways to develop these systems is to introduce methods for analyzing network traffic based on modern solutions of artificial neural network theory. To do this, it is necessary to develop a methodological framework for neural network recognition of network cyberattacks and to develop on this basis a method for creating a training sample and a method for creating appropriate neural network tools. In order to test the proposed solutions, it is advisable to develop a neural network system and conduct a study of its effectiveness.