ABSTRACT

Master's dissertation: 88 pages, 26 figures, 13 tables, 7 appendices, 22 sources.

Topicality. Information system security is extremely important today. Often there are messages in the media that the new computer virus has become a threat to the normal functioning of a large part of computers. A striking example may be the recently discovered Wanna Cry virus that affects the Microsoft Windows operating system by encrypting files.

So that, it is expedient to create a hardware and software solution that analyzes and filters traffic in real time, generates activity of devices based on packet data.

Relationship of work with scientific programs, plans, themes. The work was carried out at the Department of Computer-Aided Management and Data Processing Systems (CAMDPS) of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" within initiative theme "Methods of Visual Programming of Petri-Object Models" No. 0117U000918.

The aim of the study – improvement of the process of detecting threats from the Internet, by developing and implementing a hardware and software solution that will analyze and filter real-time traffic to find malicious signatures.

To achieve the goal you need to accomplish the following tasks:

- perform a review of the known results of solving the problem for finding threats from the Internet;
- develop software that will detect malicious traffic based on the signatures;
- to carry out an experimental study of the system functioning;
- to analyze obtained results.

The object of the study is the process of detecting malicious traffic on the devices of one subnet.

Subject of research – methods of detecting malicious traffic of devices of one subnet and its filtration.

Scientific novelty of the obtained results

An alternative architectural approach is proposed for implementing a firewall in the subnet, by running a man-in-the-middle attack. It means that there is no physical interaction of the software and hardware complex and subnet devices. The analysis of existing approaches to finding malicious traffic on devices of one subnet. Among the analyzed methods, a signature and behavioral analysis is selected. An experimental study of the obtained solution was carried out and the obtained results were analyzed.

Publications. The materials of the work are published in the theses of the All-Ukrainian Scientific and Practical Conference of Young Scientists and Students "Information Systems and Management Technologies"

PETRI NETWORKS, SYSTEM VULNARABILITY, TRAFFIC ANALYSIS, CYBER ATTACK