“SECURITY LOCATOR” – network monitoring and anomaly detection tool.

(M. Zhdanova, E. Druzhinin)

Contemporary computer networks are extremely complex in nature, integrating wide variety of telecommunicational, informational and multimedia technologies to fulfil users’ tasks. The growing involvement of computer networks in information sharing processes increases overall vulnerability to the outages of network hardware and software as a result of design/operation errors or a malicious activity. Timely detecting network malfunctions, determining and eliminating their causes can sufficiently improve the network performance and reduce possible damage from different security incidents, such as virus infections, spammer attacks, unauthorized access, denial of service, etc.

The research is focused on developing a computer-based system “SECURITY LOCATOR”, supporting continuous monitoring of network devices functioning states and automated anomaly states detection. An anomaly is understood as any deviation from the normal behavior pattern of network device, describing its standard functioning process corresponding to users’ daily activities under approved network security policy. The approach is based on network traffic processing scheme, providing accumulation and analysis of network interactions history for any period of time. The program architecture of “SECURITY LOCATOR” consists of several components: Network Agent, Data Load System, Data Visualization System and Data Analysis System. Network Agent captures, structures and accumulates structured information on network interactions as the counters for packets headers fields, grouped by a key. Developed structuring principles allow decreasing analyzed data volume to 1-5% from the initial without sufficient loss of useful information. Anomaly detection is carried out by Data Analysis System that embodies multiple data analysis modules, implementing various mathematical models. At present the abnormality level of network device current state is assigned by the modules of multidimensional statistical analysis. Detailed classification of detected anomalies is to be based on biological immune system model.

The research is carried out at Network Technologies Laboratory, organized within scientific and technical collaboration of limited company “Network Technologies Laboratory” with Moscow Engineering Physics Institute (MEPHI) and financed by The Foundation for Assistance to Small Innovative Enterprises (FASIE). The results obtained during experimental testing of “SECURITY LOCATOR” in MEPHI computer network traffic prove the effectiveness of proposed approach.