2. COMPUTER SYSTEM ANOMALOUS STATE DETECTION METHOD BASED ON FUZZY LOGIC

Chelak V., c.t.s. Gavrylenko S., Chelak E., NTU "KhPI", Kharkiv

Computer security experts agree that the amount of computer viruses and malware is growing at an alarming rate. Despite the best efforts of researchers and developers in the industry, there is currently no antivirus system that could detect one hundred percent of malicious software in existence. Thus the development and improvement of antivirus software remains a relevant problem. In the report, we look at computer system (CS) anomalous state detection methods based on fuzzy logic. In order to select the input data, we analyzed the PE structure of malicious and regular software, selected the API functions for further analysis, and evaluated them using linear programming methods. A method for identification of CS state based on Mamdani fuzzy inference system was developed. Testing of the developed identification method has shown that the probability of detecting an anomalous state, accounting for false detections, is 96.5%. Further studies of object state identification methods can be used in the study of fuzzy clustering.