СЕКЦІЯ 8. МІКРОПРОЦЕСОРНА ТЕХНІКА В АВТОМАТИЦІ ТА ПРИЛАДОБУДУВАННІ

SEMI-MARKOV MODEL FOR DEPENDABILITY ASSESSMENT OF THE INTERNET OF THINGS-BASED SMART SYSTEMS CONSIDERING VULNERABILITIES, RATES OF FAULTS OF THE SOFTWARE AND HARDWARE COMPONENTS AND RECOVERY RATES

Kolisnyk M.O.
National Technical University «Kharkiv Polytechnic Institute», Kharkiv

Internet of Things (IoT) is a system consisting of networks of sensors, actuators, and smart objects whose purpose is to interconnect “all” things, including everyday and industrial objects, in such a way as to make them intelligent, programmable, and more capable of interacting with humans and each other (IEEE). The number of devices connected to the Internet of things, growing every day. It may be smart sophisticated industrial complexes, smart transport, smart lighting systems of cities, car parks, hospitals smart, smart buildings. There are new standards and technologies to connect devices to the Internet of Things (IoT), proposed by IEEE, ISO, ANSI, IETF, 3GPP, IEC, Web of things, ITU-T, LoRa Alliance. IoT architecture intelligent system (IoTS) can be represented in the form of several layers: a three-level; four-level; five-level. The paper describes the architecture IoTS of five levels: smart connection level; data-to-information connection level; cyber level; cognition level; configuration level. Requirements to IoT: Availability, Reliability, Mobility, Performance, Management, Security and Privacy, Scalability, Interoperability.

Malicious attacks and vulnerabilities impact on components of IoTS devices, software, and databases can be applied at each of these levels. The aim of intruders can be had stored data, video and audio recordings, disabling hardware and software components IoTS, industrial espionage. To assess the reliability IoTS paper the semi-Markov model was proposed, which takes into account the different types of vulnerabilities, fails, and hardware and software failures IoTS, the recovery rate after fails and failures, as well as the malicious effects. Considering of transition from one state to another for this model takes into account the rate of attacks on vulnerabilities IoTS components, the recovery rate and the likelihood of successful attacks, the values of which are estimated based on the analysis of statistical data. The most important indicator of dependability IoTS is function of availability, which takes into account a total probability of finding the system in good working condition. In this paper was researched and analyzed function of availability of IoTS which had been received by the graph of the transition with accounting of reliability of the software and hardware components, intensity of recovery, parameters of vulnerabilities.

The method of IoTS dependability evaluation, based on semi-Markov model was proposed.