

Informatika i sistemy upravleniya. – 2020. – No. 3(65). – P. 3-13.

Voronin V.V. (004183@pnu.edu.ru), **Morozov A.V.**
Pacific State University

MALICIOUS SOFTWARE SECURITY THREAT CONTROL METHOD

The article discusses data processing methods and the construction of neural network architectures to perform behavioral analysis of malicious software. A research of the methodology for detecting security threats based on the obtained architectures of neural networks has been carried out. Conclusions have been made about the data requirements within the problem under consideration and about the effectiveness of the proposed methodology.

Keywords: security threats, behavioral analysis, API calls, malware, neural network, machine learning, LSTM, CNN.

DOI: 10.22250/isu.2020.65.3-13

For citation:

Voronin V.V., Morozov A.V. MALICIOUS SOFTWARE SECURITY THREAT CONTROL METHOD // Informatika i sistemy upravleniya. – 2020. – No. 3(65). – P. 3-13.