DEVELOPMENT OF THE MALWARE DETECTION SYSTEM BASED ON THE NEURAL NETWORK

Gavrylenko S., Babenko O.
National Technical University «Kharkiv Polytechnic Institute», Kharkiv

It is known that over a year, viruses cause damage to hundreds of billions of dollars, and about the same amount is indirect damage associated with the development of software and other measures to protect against viruses. That is why the actual topic is the development of effective methods and technologies for counteracting computer viruses based on heuristic methods [1-5]**.**

In this report the PE structure of malicious and secure software is analyzed, features are highlighted, binary sign vectors are obtained and used as inputs for training the neural network.

The software model of the heuristic analyzer on the basis of the ART-1 neural network has been developed, the optimal similarity coefficients were found, and the tested computer virus detection system was tested.

The results of the identification system showed that when training the neural system by the Backdoor sample, the system also begins to identify harmful Trojan (28%) signatures, since these types of signatures have a high similarity coefficient, since they perform similar actions from the point of view of the operating system.

When learning a worm-patterned system, only a signature of this type is detected, due to a relatively high optimal similarity factor of 0.97, the tokens of this type are abandoned from Signature Backdoor, Trojan, and secure software. Also, when training a neural system with Trojan sampling, in addition to this sample, the system recognizes backdoor signatures (46%) and insignificant number of worm-signatures (1%). This percentage of signature recognition (Backdoor - Trojan and vice versa) is due to the fact that these types of viruses have similar actions from the point of view of the operating system namely harm to it: the desire to obtain unauthorized access to data or remote control of the operating system and the computer as a whole.

References:

1. Lukatsky A.V. Attack Detection / Lukatsky A.V. – St. Petersburg: VHV-Petersburg, 2001.– 624 p.

2. Shelukhin O.I. Intrusion Detection into Computer Networks / Shelukhin O.I., Sakalema D.Zh., Filinov A.S. – Moscow: Hot line-Telecom, 2013. – 220 p.

3. Gavrilenko S. Development of templates for the identification of the state of computer systems based on BDS-testing / Semenov S., Gavrilenko S., Chelak V. // Bulletin of NTU "KhPI". Informatics and modeling . – Kharkov, 2016. – № 21. – P. 118-125.

4. Gavrilenko S. Intrusion detection in computer systems / Gavrilenko S., Chelak V., Hornostal O. //Proceedings of the symposium "Metrology and metrology assurance". – Sozopol, Bulgaria, 2016. – P. 342-347.

5. Semenov S. Developing parametrical criterion for registering abnormal behavior in computer and telecommunication systems on the basis of economic test // Semenov S., Gavrilenko S., Chelak V. //Actual problems of economics. – Kiev, 2016. – Vol 4 (178). – P. 451-459.