Method of neural networks utilization for malware recognition

UDC 004.056.5 Volodymyr Pogorelov[1], Mykolay Karpinski[2],

Evheniia Ivanchenko[3]

National Aviation University[1,3], Akademia Techniczno-Humanistyczna

w Bielsku-Białej[2], [1]volodymyr.pogorleov@gmail.com, [2]mpkarpinski@gmail.com, [3]evivancenko@gmail.com

An important way to improve the recognition of computer viruses is the "intellectualization" of recognition methods through the use of the theory of artificial neural networks (NN). The prospects of this area are confirmed by some successful applications of NN in the detection of computer viruses (antivirus with open source ClamAV, startup Deep Instinct) and a large number of relevant theoretical and practical work. However, insufficient recognition accuracy and insufficient adaptability to operating conditions, the secrecy of the solutions used significantly limit their scope. At the same time, constant progress in the field of neural network theory indicates the possibility of significant improvement of the tested recognition methods.

In such a setting, the scientific and applied task of developing an effective neural network method for recognizing computer viruses, adapted to the conditions of domestic anti-virus protection systems, is relevant.

The proposed method consists of the following steps:

Stage 1 - determining the conditions for the creation and use of NN.

Stage 2 - the formation of portraits of viruses and secure programs.

Stage 3 - determination of architectural parameters of DNN.

Stage 4 - verification of NN.

Stage 5 - evaluation of the effectiveness of NN.

The computer virus database BIG-2015, published by Microsoft, is used for training and testing of DNN (table 1).

Table 1

Database BIG-2015

Name	*Number of examples*
Ramnit	1541
Lollipop	2478
Kelihos_v3	2942
Vundo	475
Simda	420
Tracur	751

Note that due to the use of the proposed design method GNM architecture managed to avoid long-term numerical experiments, aimed at determining the appropriateness of its use and to determine it structural parameters, and approximately 1.5 times to reduce computational costs, related to the definition of the specified architectural parameters.

Thus, the results studies confirm the possibility of improving the efficiency of recognition computer viruses through the application of the developed method.

Supervisor — doctor of science, prof., Terejkowskyi I.A

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ

X міжнародної науково-технічної конференції «ITSec»

19-24 березня 2020 року

м. Київ (Україна), м. Шарм-ель-Шейх (Египет),
Національний авіаційний університет

Оригінал-макет підготовлено на кафедрі
безпеки інформаційних технологій
Національного авіаційного університету