Annotation

of dissertation for the degree of Philosophiae Doctor (PhD) on the specialty 6D070300 Information Management System

IDEYAT BAPIYEV

Neutral network models and attacking counteracting methods against the network resources information systems

Urgency of the research. The main threats to sustained and safe operations of the national information systems are manifestations of computer crimes and terrorism, according to the cybersecurity concept «Kiberschit Kazakhstana (Kazakhstan's Cyberboard)» [1]. Network attacks counteracting systems are an essential tool of information security of the network resources information system, in the modern world. Although such systems are used for more than a decade, many qualified specialists are involving in developing and a large number of works have been devoted to the creation of an appropriate scientific and methodical framework, however practical experience shows a number of major deficiencies in the network cyber-attacks counteracting system. The main one is lack of precision of recognition of all network cyber-attacks nomenclature that is confirmed by known cases of successful unauthorized access to information security systems in some countries. Besides that, implementation of known network cyber-attacks counteraction methods inside the information security system of the domestic information systems necessitating of its difficult adaptation to variability of terms of use. Also the deficiencies of known counteracting methods of attacking the network resources information system are the high cost and lack of detailed scientific and technical documentation.

In that case, the actual task is developing effective network cyber-attacks counteraction models, methods and systems that would be adapted to domestic terms of use.

Scientists research such as V.I Vassilyev [3], A.V. Grishin [4], Yu.G. Yemelyanova [5], A.V. Kryzhanovski [8], A.G. Mustafayev [9], I.I. Slepovichev [10], A.A. Talalayev [12] and the others show that the use of the neural simulation device is a promising way to increase the cyber-attacks recognition. This is explained by the proven efficacy of using the neural networks to solve these problems by the leading developers of the information security facilities (Cisco and Symantec) and proven adaptability of neural network means to a wide variety terms of use.

The theoretical development and information security systems implementation experience of such scientists as B.B. Akhmetov [2], A.A. Korchenko [6], V.E. Sukhov [11], I.A. Tereikovski [13], A. Timofeev [14], S.T. Tynynbayev [7], A.F. Khafizov [15], V.A. Chastikova [16] and the other, is the methodological and theoretical basis for effective implementation of the neural network means inside the attacks counteracting systems.

Thus, the task of developing effective neural network cyber-attacks countering models, methods and means against the network resources information systems determines the relevance of scientific research and development the dissertation work is focused.

Aim and objectives of the research. The aim of the dissertation work is develop effective neural network cyber-attacks countering models, methods and tools adapted to operating conditions and capable quickly recognizing new types of cyber-attacks.

In accordance with the aim, the following research objectives are defined:

– to analyze the capabilities of neural network cyber-attacks countering against the network resources information systems;

– to develop the methodological framework of neural network cyber-attacks counteraction against the network resources information systems;

– to develop neural network cyber-attacks countering models and methods;

– to develop a neural network cyber-attacks countering network and carry out experimental research for verifying the proposed solutions.

The object of research is the processes of cyber-attacks countering against the network resources information systems.

The subject of the research is the neural network cyber-attacks countering models, methods and means against the network resources information systems.

Methods of research - methods of the theory of digital signal processing, neural networks, expert analysis, mathematical statistics and optimization.

The scientific novelty of the results is the theoretical and practical research allowed for the development and provide a scientific base of the principles, neural network cyber-attacks counteraction models and methods against network resources information systems.

For the first time:

– a method of creating a training sample for neural network cyber-attacks counteraction have been developed that helps to determine the range of permissible types of neural network models and to reduce the number of training iterations by identifying the parameters of permissible sampling types and taking into account the proximity of standards of cyber-attack in the output signal;

– a method of neural network cyber-attacks counteraction against the network resources information systems have been developed that allows to expand the functionality and provide sufficient recognition accuracy by using of developed neural network models and the developed method of creating a training sample.

Further development have received:

– the methodological framework of neural network cyber-attacks counteraction against network resources information systems that ensured the possibility of creating effective neural network counteraction models and methods due to the conditions for the creation of these means;

– the neural network countermeasures models allows a rapid response to new types of network cyber-attacks due to the possibility of training with the help of expert data and use of a combined training sample.

Practical importance of the results. The proposed neural network models and methods allowed to develop the neural network system architecture that allows to identify the main types of network cyber-attacks with sufficient precision and can also be used to create the device tools adapting to the conditions of creation and operation.

Practical importance is:

– using of the developed method of creating a training sample allows to reduce the number of the neural network model training iterations approximately in 2.4 times that confirmed by the act of introducing into the work of “Tezis” the Research Center of Kyiv Polytechnic Institute after I. Sikorski (the act dated 11.09.2017);

– application of the developed neural network method of network cyber-attacks recognition allows to increase the efficiency of neural network tools for recognizing network cyber-attacks approximately in 1.35 times that confirmed by the act of introducing into the work of “Delta” Bezopasnost Informatsionnyh Sistem, OOO (the act dated 09.10.2017);

– the developed programs that implement the proposed models and methods, introduced into the educational process at the Department of Information Technology Security Department of National Aviation University (Kyiv, Ukraine, (the act dated 25.07.2017) and at the Department of Information Systems of West Kazakhstan Agrarian and Technical University after Zhangir Khan (the act dated 04.09.2017).

Personal contribution of the degree-seeking student. The works have been published in coauthored and the degree-seeking student has the following works: development of the new method of creating a training sample for neural network cyber-attacks counteraction developed that helps to determine the range of permissible types of neural network models and to reduce the number of training iterations approximately in 2.4 times by identifying the parameters of permissible sampling types and taking into account the proximity of standards of cyber-attack in the output signal; development of the method of neural network cyber-attacks counteraction against the network resources information systems that allows to expand the functionality and provide sufficient recognition accuracy of the network cyber-attacks by using of developed neural network models and the developed method of creating a training sample. The neural network cyber-attacks countering system against network resources information systems was developed and investigated by using the proposed models and methods. This system provides for the use of subsystems for determining the terms for creating neural network facilities, formation of an adaptive learning sample and the neural network models development providing sufficient recognition accuracy and adaptation to the terms of development and application, unlike well-known neural network facilities. By an experimental way, the efficiency of the proposed neural network system is higher at approximately 1.35 times relevant to the best similar systems and under the expected application conditions, its use will allow an error of recognizing network cyber attacks within the range of 0.05, which is sufficient for practical use.

Evaluation of results: The main results of the dissertation were reported and discussed at the seminars of the department "Information Technologies" of Kazakh National Research Technical University after K.I. Satpaev and at international scientific and practical conferences:

– II International Research and Practical Conference «Cyber and information security current issues», European University (Kyiv, Ukraine, 24-27 of February 2016);

– III International Research and Practical Conference «Cyber and information security current issues», European University (Kyiv, Ukraine, February 22-25 of February 2017);

– IV International scientific conference «Global and regional problems of informatizition in society and nature using'2016», Ukraine National University of Life and Environmental Sciences (Kyiv Ukraine, 23-24 of June 2016);

– V International scientific conference «Global and regional problems of informatizition in society and nature using'2017», NULES of Ukraine (Kyiv, Ukraine, 22-23 of June 2017);

– The 15th International Scientific Conference Information Technologies and Management, ISMA University – Satpayev University, (Latvia - Kazakhstan, Riga - Almaty, April 27-28, 2017);

– Safety improvement of the information and telecommunication systems (SITS'2017), Nikolayiv – Koblevo: Nikolaiyvska Politekhnika, International University of Technology (Nikolayiv – Koblevo, Ukraine, 20-23 of June 2017).

Contributions. The main results obtained in the performance of the dissertation were published in 14 publications, of which 4 articles were published in the publication recommended by the Control Committee in Education and Science under the Ministry of Education and Science of the Republic of Kazakhstan, 1 article was published in the publication indexed by the Scopus database, 1 article was published in the international journal (Academy of Natural History), 1 article was published in a foreign journal (Ukraine), 6 articles were published in foreign publications of international scientific and practical conferences (Ukraine, Latvia), 1 article was published in the domestic publication of the international scientific-practical conference (Kazakhstan).

The volume and structure of the thesis. The dissertation has the introduction, four main sections, conclusion and the list of used sources, 106 titles and 6 appendixes. The total amount of dissertation is 124 pages. The work contains 25 illustrations and 7 tables.

USED SOURCES

1. Cybersecurity concept "Kiberschit Kazakhstana" approved by Kazakhstan Government Decision No 407 of 30 June 2017, [Electronic information database]- http://mdai.gov.kz/ru/pages/ koncepciya-kiberbezopasnosti-kibershchit-kazahstana (date 16.12/2017)

2. B.B. Akhmetov Parameters of evaluating the effectiveness of neural network tools for cyber-attacks recognizing against network resources information systems /B.B. Akhmetov, A.G. Korchenko, I.A. Tereikovski, Zh.M. Alibiyeva// Reports of the national academy of sciences of the Republic of Kazakhstan. ISSN 2224-5227. Volume 2, Number 312 (2017)

3. V.I. Vassilyev. Neural networks in detection network Internet attacks (example SYNFLOOD attacks)/ V.I. Vassiliyev, A.F. Khafizov // Neurocomputers in information and expert systems. – M.: Padiotechnika, 2007. – No 6. – p. 34-38.

4. A.V. Grishin Neural network technologies in the tasks of computer attacks detecting / A. V. Grishin // Information technology and computer systems
– 2011. – №1. – p. 53 - 64.

5. Yu.G. Yemelyanova, Neural network technology of detecting network attacks against information resources / Yu. G. Yemeliyanova, A.A. Talalayev, I. P. Tischenko, V.P. Fralenko// Software systems: theory and applications – 2011. – No 3(7). – p. 3-15.

6. A.G. Korchenko. Determination of effective types of the neural network models for cyber-attacks recognizing against network resources/ A.G. Korchenko, I.A. Tereikovski, I.A. Tereikovskaya, L.A. Tereikovskaya, B.B. Akhmetov// Legal, normative and metrological provision of the information security system in Ukraine, red. 2 (32), 2016.

7. A. G. Korchenko Neural network models, methods and tools for evaluating security parameters of Internet-oriented information systems: monograph / A. Korchenko, I. Tereikovski, N. Karpinski, S. Tynymbayev – К. : TOV "Nash Format" – 2016. – p. 275.

8. A.V. Kryzhanovski Artificial neural networks application against attack detection systems / A.V. Kryzhanovski //Tomsk State University of Control Systems and Radioelectronics Reports. – 2008. – No 2 (18), Part 1. – p. 37-41. URL: https://cyberleninka.ru /article/n/primenenie-iskusstvennyh-neyronnyh-setey-v-sistemah-obnaruzheniya-atak

9. A.G. Mystafayev Computer attacks neural network detection based on network traffic analysis// Security issues. – 2016. – No 2. – p.1-7. DOI: 10.7256/2409-7543.2016.2.18834. URL: http://e-notabene.ru /nb/article_18834.html.

10. I. I. Slepovichev DDoS-attacks detection using the fuzzy neural network / I. I. Slepovichev, P.V Irmatov, M.S. Komarova, A.A. Bezhin// Izvestiya of Saratov University . – 2009. – T. 9, ser. Mathematics. Mechanics. Computer science, red.. 3. – p. 84-89.

11. V.E. Sukhov Network traffic anomalies detection system based on artificial immune systems and neural network detectors // Ryazan State Radio Engineering University Vestnik. – 2015. – No 54. Part.1. – p. 84-90.

12. A.A. Talalayev Neural network monitoring abnormal network activity development module/ A.A. Talalayev, I.P. Tischenko, V.P. Fralenko, V.M. Khachumov// Neurocomputers: Development and Application. — 2011. — No 7. — p. 32-38.

13. I. Tereikovski Neural networks in the means of computer information protection: monograph / I. Tereykovsky. – K.: PolygraphConsulting . – 2007. – p-209.

14. A. Timofeev Investigation and simulation of the neural network detection method and network attacks classification/ A. Timofeev, A. Branitski // Information Technologies & Knowledge International Journal. – 2012. – Vol.6, Number 3. – P. 257-265

15. A.F. Khafizov, Neural network detecting attacks on the WWW server: dissertation work. … Candidate of technic sciences: 05.13.11 / A.F. Khafizov. – Ufa, 2004. – p. 172.

16. V.A. Chastikova, K.A. Vlasov, D.A. Kartamyshev Ddos attacks detection based on neural networks using the particle swarm method as a learning algorithm/ V.A. Chastikova, K.A. Vlasov, D.A. Kartamyshev // Fundamental research – 2014. – No 8-4. – p. 829-832.