tack, if any (each of these four neural networks corresponds to one class of attack and is able to identify types that belong only to this class). **Findings.** The created software model was used to study the parameters of the neural network configuration 41–1–132–5, which determines the category of the attack class on the computer network. It is determined that the optimal training speed is 0.001. The ADAM algorithm proved to be the best for optimization. The ReLU function is the most suitable activation function for the hidden layer, and the hyperbolic tangent function – for the output layer activation function. Accuracy in test and validation samples was 92.86 % and 91.03 %, respectively. **Originality.** The developed software model, which uses the Python 3.5 programming language, the integrated development environment PyCharm 2016.3 and the Tensorflow 1.2 framework, makes it possible to detect all types of attacks of DoS, U2R, R2L, Probe classes. **Practical value.** Graphical dependencies of accuracy of neural networks at various parameters are received: speed of training; activation function; optimization algorithm. The optimal parameters of neural networks have been determined, which will ensure a sufficiently high level of reliability of intrusion detection into a computer network.

Keywords: architectural solution; neural network; training speed; activation function; optimization algorithm

REFERENCES

1. Branitskiy, A. A. (201_). *Obnaruzhenie anomalnykh setevykh soedineniy na osnove gibridizatsii metodov vychislitelnogo intellekta* (Extended abstract of PhD dissertation). St. Petersburg, Russia. (in Russian)
2. Zhulkov, Ye. V. (2007). *Postroenie modulnykh neyronnykh setey dlya obnaruzheniya klassov setevykh atak* (Extended abstract of PhD dissertation). St. Petersburg, Russia. (in Russian)
3. Pakhomova, V. M., & Konnov, M. S. (2020). Research of two approaches to detect network attacks using neural network technologies. *Science and Transport Progress, 3*(87), 81-93. DOI: https://doi.org/10.15802/stp2020/208233 (in Ukrainian)
4. Frolov, P. V., Chukhraev, I. V., & Grishanov, K. M. (2018). Application of artificial neural networks in intrusion detection systems. *System administrator, 9*(190). Retrieved from samag.ru/archve/article/3724 (in Russian)
5. Amini, M., Rezaeenour, J., & Hadavandi, E. (2014). A Neural Network Ensemble Classifier for Effective Intrusion Detection Using Fuzzy Clustering and Radial Basis Function Networks. *International Journal on Artificial Intelligence Tools, 25*(02), 1-32. DOI: http://doi.org/10.1142/s0218213015500335 (in English)
6. Esteban, J. (2008). A New GHSOM Model applied to network security. *Artificial Neural Networks-ICANN 2008* (pp. 680-689). (in English)
7. Grill, M., Pevný, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences, 83*(1), 43-57. DOI: https://doi.org/10.1016/j.jcss.2016.03.007 (in English)
8. Hadi, A. A. A. (2018). Performance Analysis of Big Data Intrusion Detection System over Random Forest Algorithm. *International Journal of Applied Engineering Research, 13*(2), 1520-1527 (in English)
9. KDD Cup 1999 Data. Retrieved from http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (in English)
10. Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing, 172*, 385-393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101 (in English)
11. Sikos, L. F. (2018). *AI in Cybersecurity*. New York: Springer. (in English)
12. TensorFlow. Retrieved from http://www.tensorflow.org (in English)
13. Zhukovyts'kyy, I. V., & Pakhomova, V. M. (2018). Identifying threats in computer network based on multilayer neural network. *Science and Transport Progress, 2*(74), 114-123. DOI: https://doi.org/10.15802/stp2018/130797 (in English)
14. 2018 Data Breach Investigations Report. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (in English)

Надійшла до редколегії: 28.05.2020
Прийнята до друку: 28.09.2020

doi: https://doi.org/10.15802/stp2020/218318