https://www.proconference.org/index.php/gec/article/view/gec29-01-019
DOI: 10.30890/2709-1783.2023-29-01-019

UDC 004.056.53:[004.7:004.032.26]

METHODS OF FORMING COMPETENCIES IN APPLICANTS FOR THE SPECIALTY «CYBERSECURITY» WHEN PERFORMING A COURSE ASSIGNMENT IN THE DISCIPLINE «LOCAL NETWORKS»

МЕТОДИКА ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ У ЗДОБУВАЧІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» ПРИ ВИКОНАННІ КУРСОВОГО ЗАВДАННЯ З ДИСЦИПЛІНИ «ЛОКАЛЬНІ МЕРЕЖІ»

Pakhomova V. M. / Пахомова В. М.
c.t.s., as. prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Ukrainian State University of Science and Technology,
Ukraine, Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій,
Україна, Дніпро, вул. Лазаряна, 2, 49010

Abstract. *The methodology of «AttackDetectionLAN» for the formation of professional and subject competencies of applicants for the degree «Bachelor» in the specialty «Cybersecurity» in the course assignment in the discipline «Local Networks» is proposed: 1) obtaining an idea of the network categories of attacks and the corresponding network classes of attacks; 2) configuration of a multilayer neural network to detect network attacks; 3) creation of a neural model in accordance with the composite structure using the selected neuropackage; 4) on the basis of an open NSL-KDD database, preparation of samples for training and testing of the created neural network; 5) determination of the optimal parameters of the created neural network.*

Keywords: *competence, course task, network attack, neural network, configuration, sampling, activation function, learning algorithm, error.*

Анотація. *Запропонована методика «AttackDetectionLAN» щодо формування фахових та предметних компетентностей здобувачів ступеня «бакалавр» спеціальності «Кібербезпека» при виконанні курсового завдання з дисципліни «Локальні мережі»: 1) отримання уявлення про мережеві категорії атак та відповідні до них мережеві класи атак; 2) складання конфігурації багатошарової нейронної мережі щодо виявлення мережевих атак; 3) створення нейронної моделі відповідно до складеної структури за допомогою обраного нейропакету; 4) на основі відкритої бази даних NSL-KDD підготовка вибірок для навчання та тестування створеної нейронної мережі; 5) визначення оптимальних параметрів створеної нейронної мережі.*

Ключові слова: *компетентність, курсове завдання, мережева атака, нейронна мережа, конфігурація, вибірка, функція активації, алгоритм навчання, похибка.*

Entry

Statement of the problem. The current state in the world, which is associated with the spread of infected diseases and military events that threaten the lives of applicants, has led to the use of blended learning, in particular in the discipline «Local Networks», as well as the formation of relevant professional and subject competencies in applicants for a bachelor's degree under such difficult conditions of our time, which confirms the relevance of the topic.

Analysis of the latest research. Competency assessment is the subject of research by many scientists. It is important to identify, analyze and summarize the experience of EU countries, important international organizations and initiatives (UNESCO, ECDL, MICROSOFT, INTEL, etc.), as well as comparability for modern Ukrainian education in international studies of the quality of education (PISA,

TIMSS, PEARLS) [1]. The analysis of recent studies and publications revealed the following: 1) lack of unified information and communication technologies for teaching in the discipline «Local Networks»; 2) the need for timely detection of network attacks based on the use of neural network technology; 3) the existence of a wide range of neuropackages suitable for creating a neural network (NN); 4) features of Generation Z, and became the basis for the development of its own methodology.

The aim of the article is to develop the «AttackDetectionLAN» methodology for the formation of professional and subject competencies in applicants for the degree of «Bachelor» in the specialty «Cybersecurity» when performing a course assignment in the discipline «Local Networks».

General characteristics of the «AttackDetectionLAN» technique. The proposed «AttackDetectionLAN» technique provides an opportunity for first-degree students in the discipline «Local Networks»: to get an idea of the network categories of attacks and the corresponding network classes of attacks; configure a multilayer NN to detect network attacks; create an NN according to the composite structure using the selected neuropackage; based on the NSL-KDD (or KDDCup) database, prepare samples for training and testing the created NN; investigate the optimal parameters of NN.

Network categories and attack classes. The DoS category is characterized by generating a large amount of traffic, which leads to server overload and blockage. The following classes of network attacks are known according to the DoS category: Back; Land; Neptune; Pod; Smurf; Teardrop. The PROBE network category is aimed at scanning ports in order to obtain sensitive information. The main network classes of PROBE attacks are: Ipsweep; Nmap; Portsweep; Satan. The category of R2L network attacks is characterized by the acquisition of access by an unregistered user to a computer from a remote computer. The R2L category includes the following network attack classes: Ftp_write; Guess_passwd; Imap; Multihop; Phf; Spy; Warezclient; Warezmaster. U2R network attacks are system attacks in which a hacker runs a system with a regular user account and tries to exploit vulnerabilities in the system to gain superuser privileges. The main network classes of U2R attacks are: Buffer overflow; Loadmodule; Perl; Rootkit.

Multilayer perceptron as the main method. To detect network attacks, it is advisable to use neural network technology, in particular MLP (Multi Layer Perceptron). As an example, the MLP structure for detecting network attacks of the PROBE category is presented (Figure 1).

The first layer of NN has X1... X41 neurons (these are the parameters of network traffic) [3]. The resulting layer has the following neurons: Y1 – Normal (normal state: no attack on the local network); Y2 – Nmap-class attack; Y3 – Satan-class attack; Y4 – Ipsweep-class attack; Y5 – Portsweep-class attack.

Sampling and creation of NN. Based on the NSL-KDD database [3], a sample of 250 examples was compiled (50 examples for each network class and its absence), an excerpt of which is presented in Table 1 as an example.

With the help of the Toolbox package, MatLAB created the NN configuration 41-1-20-5, where 41 is the number of neurons of the first layer (network traffic parameters), 1 is the number of hidden layers, 20 is the number of hidden neurons, 5 is the number of resulting neurons; a hyperbolic tangent is taken as the activation

function of the hidden layer, and a linear function is taken on the resulting layer. Created in MatLAB NN, the structure of which is shown in Figure 2; the obtained results (regression values) on the generated NN are shown in Figure 3.

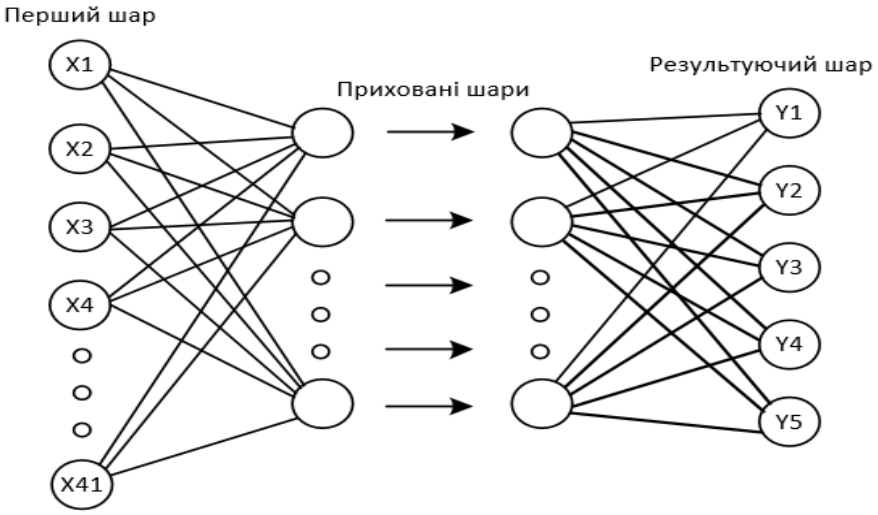

Figure 1 – Structure of a MLP [2]

Table 1 – Sample fragment (for first-layer neurons) [2]

X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	...	X41
0	2	1	1	8	0	0	0	0	0	9	...	0
0	1	2	2	0	0	0	0	0	0	0	...	1
0	2	1	1	8	0	0	0	0	0	0	...	0
...	...	...	...	...	...	...	...	...	...	...	...	...

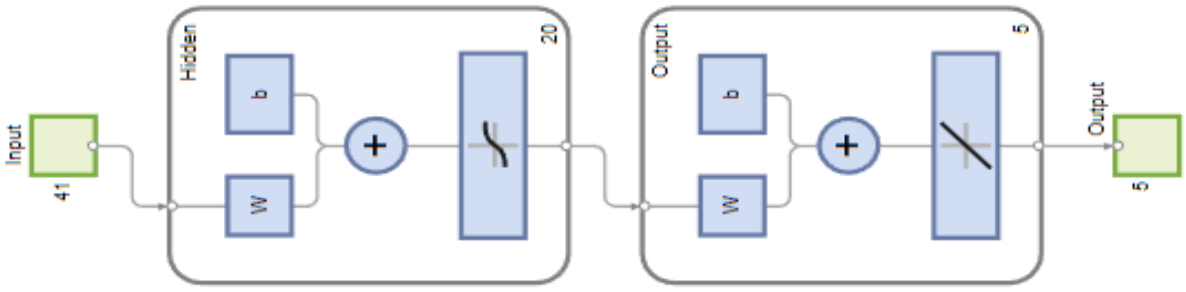

Figure 2 – Structure of the created NN in MatLAB [2]

Determination of optimal NN parameters. On the created NN, an error study (Mean Square Error, MSE) was carried out with a different number of hidden neurons (20, 40, 60 and 80) using the following NN learning algorithms: Levenberg-Marquardt; Bayesian regularization; Scaled Conjugate Gradient) on samples of different lengths (250, 750, and 1500 examples). It was determined that the smallest value of the NN error was 0.0071 with 60 hidden neurons according to the Levenberg-Marquardt learning algorithm on a sample of 1500 examples (300 examples for each network class).

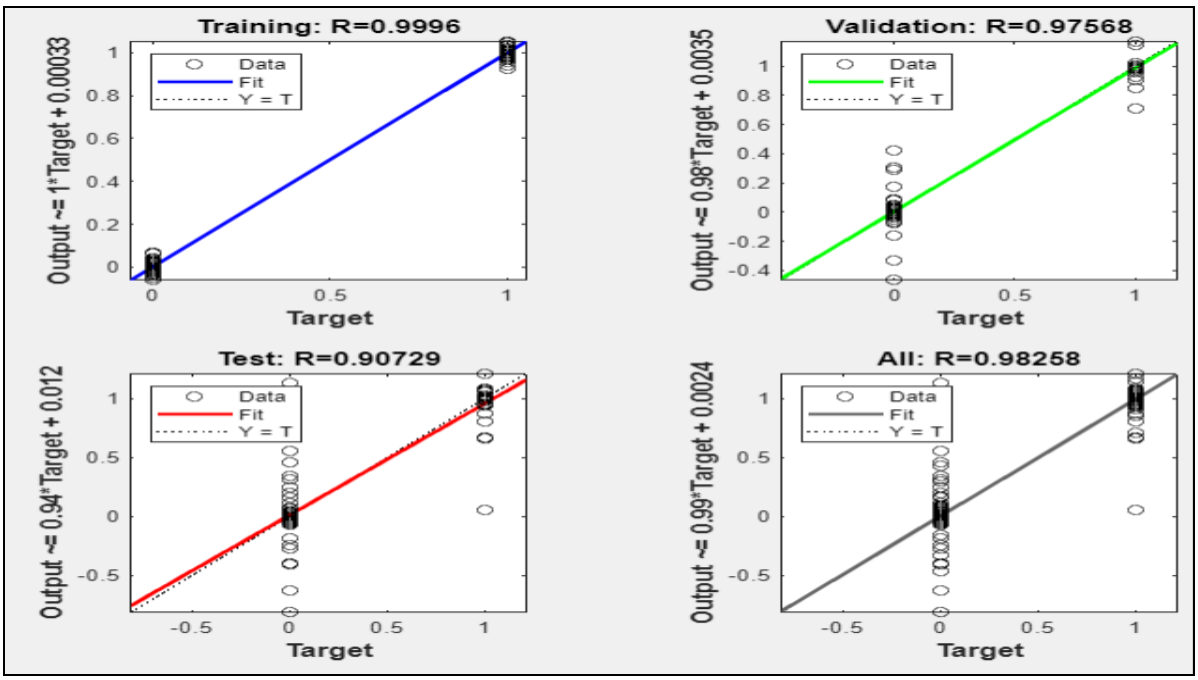

Figure 3 – Results obtained on NN configuration 41-1-20-5 [2]

Conclusions

1. The proposed methodology of «AttackDetectionLAN» for the formation of professional and subject competencies in applicants for the degree «Bachelor» in the specialty «Cybersecurity» in the course assignment in the discipline «Local Networks»: 1) obtaining an idea of the network categories of attacks and the corresponding network classes of attacks; 2) configuration of multilayer NN to detect network attacks; 3) creation of NN in accordance with the composite structure with the help of the selected neuropackage; 4) on the basis of the open database NSL-KDD, preparation of samples for training and testing of the created NN; 5) determination of the optimal parameters of the created NN.

2. Based on the use of the «AttackDetectionLAN» methodology, the applicant for a bachelor's degree in the specialty «Cybersecurity»: firstly, masters professional competencies in the specialty «Cybersecurity»; secondly, mastering subject competencies in the discipline «Local Networks»; thirdly, acquires practical skills in scientific activities while conducting research on the optimal parameters of the created model of multilayer NN.

Literature:

1. Биков В. Ю., Овчарук О. В. Оцінювання інформаційно-комунікаційної компетентності учнів та педагогів в умовах євроінтеграційних процесів в освіті: посібник. Київ: Педагогічна думка, 2017. 160 с.

2. Пахомова В. М., Квочка М. Ю. Визначення мережевих атак категорії PROBE засобами багатошарової нейронної мережі. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 34(73). № 4, 2023. С. 93-98.

3. NSL-KDD dataset. UNB: веб-сайт. URL: https://www.unb.ca/cic/datasets/nsl.html (дата звернення: 05.05.2023).