Detection Of Intrusion Attacks Using Neural Networks

Mikolaj Karpinski[1], Alexander Shmatko [2], Serhii Yevseiev[3], Daniel Jancarczyk[4] and Stanislav Milevskyi[5]

[1,4] *University of Bielsko-Biala, Department of Computer Science and Automatics, Willowa Str. 2, Bielsko-Biala, 43-309, Poland*
[2,3,5] *Simon Kuznets Kharkiv National University of Economics, Cybersecurity and Information Systems Department, ave. Science, 9-A, Kharkiv, 61166, Ukraine*

Abstract
The rapid expansion of computer networks makes security issues among computer systems one of the most important. Intrusion detection systems are using artificial intelligence more and more. This article discusses intrusion detection. Multi-layer perceptron (MLP) is used to detect offline intrusion attacks. The work uses the issues of determining the type of attack. Various neural network structures are considered to detect the optimal neural network by the number of input neurons and the number of hidden layers. It has also been investigated that activation functions and their influence on increasing the ability to generalize a neural network. The results show that the neural network is a 15x31x1 way to classify records with an accuracy of about 99% for known types of attacks, with an accuracy of 97% for normal vectors and 34% for unknown types of attacks.

Keywords
detection of anomalies, expert systems, neural networks, intrusion detection system, network attacks.

1. Introduction

Currently, information technology has penetrated practically all spheres of life of modern society. And an integral part of information technology is the Internet. The reason for such an intensive development of information technology is the growing need for quick and high-quality processing of information, the instantaneous transmission of information to various parts of the world. In this regard, one of the main tasks is to ensure the security of information that is transmitted or processed on the network, protection against network attacks.

At the moment, complex information security systems are becoming increasingly important. As components of such system act as antivirus protection systems, integrity monitoring systems, firewalls, vulnerability analysis, detection and prevention systems, etc. Intrusion Detection and Intrusion Detection Systems, or, as they are called, the means of detecting attacks, is precisely this mechanism of protection of the network, which is assigned the functions of protection against network attacks.

There is a large number of methods for detecting network attacks, but as attacks constantly change special databases with rules or signatures to detect attacks requiring continuous administration, there is a need to add new rules. One of the ways to eliminate this problem is to use the neural network as a mechanism for detecting network attacks. Unlike the signature approach, the neural network performs an analysis of information and provides information about the attacks that it is trained to recognize. In addition, neural networks have the advantage - they are able to adapt to previously unknown attacks and detect them [1-3].

EMAIL: mkarpinski@ath.bielsko.pl (A.1),
asu.spios@gmail.com, (A.2), Serhii.Yevseiev@hneu.net, (A.3),
djancarczyk@ath.bielsko.pl (A.4),
Stanislav.Milevskiy@hneu.net (A.5)
ORCID: 0000-0002-8846-332X (A.1), 0000-0002-2426-900X (A.2), 0000-0003-1647-6444 (A.3), 0000-0003-4370-7965 (A.4), 0000-0001-5087-7036 (A.5)

2. Analysis of existing methods for intrusions detecting

Detecting network attacks is a process of recognizing and responding to suspicious activity directed to the network or computing resources of an organization [3]. From what information analysis methods are used for analysis, the effectiveness of the technology of detecting network attacks strongly depends on. Currently, there are many methods for detecting attacks, let's consider some of them.

Behavioral methods are called methods based on the use of information about the normal behavior of the system and its comparison with the parameters of observable behavior [1]. The presented group of methods is oriented on the construction of a standard, or normal, system or user system. In the course of their work, systems that use this approach compare current activity figures with a profile of normal activity, and the case of significant deviations can be considered as evidence of an attack. These methods are characterized by the presence of false positives, which are explained primarily by the complexity of the exact and complete description of the plurality of legitimate user actions. In addition, for most such systems, it is necessary and necessary to carry out the stage of the previous setting, during which the system "gaining experience" to create a model of normal behavior. The length of this interval for data collection may take several weeks, and sometimes a few months. These disadvantages are often the main reasons for the refusal to use systems based on behavioral methods in favor of systems that use accurate representation of network security breaches. One of the behavioral methods is statistical analysis.

Statistical analysis is the core of methods for detecting anomalies in the network. At the very beginning of this method, profiles are defined for each subject of the analyzed system. Any deviation of the profile used from the reference is considered to be unauthorized activity. [2]

It should be noted that in the statistical systems an important role is played by the correct choice of controlled parameters that characterize the differences in normal and abnormal traffic. It may turn out that due to the wrong choice of the number of observed parameters, the model describing the behavior of entities in the system will be incomplete or excessive. This results in the passage of attacks or false alarms in the system.

The advantages of statistical systems are their adaptation to change the behavior of the user, as well as the ability to detect the modifications of the attack. Among the shortcomings

it is possible to note the high probability of occurrence of false reports of attacks, as well as their pass.

Knowledge-based methods include such methods, which in the context of the given facts, rules of output and comparison, reflect the signs of given attacks, produce actions to detect attacks based on the found mechanism of search [4]. As a search procedure, a pattern matching, a regular expression machine, a logical sequential conclusion, a state transition, etc. can be used. Their name implies that systems based on their application work with a knowledge base, including information about already known attacks. Here the knowledge base is represented by a repository containing expert records supporting the logic of their processing and interpretation (that is, it is characterized by the presence of a subsystem of logical output). If there is no precise knowledge about the modification of the harmful activity, then these methods can not cope with the detection of various variations of this harmful activity. The group of data methods includes signature methods.

In signature methods, system events are presented in the form of strings of characters from a certain alphabet. The essence of these methods is to set the set of attack signatures in the form of regular expressions or patterns based on model matching and verify the match of the observed events with these expressions. Signature is a set of attributes that can distinguish network attacks from other types of network traffic. In the input package, the byte is viewed by byte and compared to the signature (signature) - a characteristic line of the program, indicating the characteristics of malicious traffic. Such a signature may contain a key phrase or a command that is associated with an attack. If a match is found, an alarm is announced [4].

The main advantage of the signature method is that the detection of known samples of abnormal events is carried out as effectively as possible. But at the same time, the use of a signature database of a large volume negatively affects the performance of the detection system. The disadvantage of this method is the impossibility of detecting attacks whose signature has not yet been determined.

Methods of computing intelligence. This category includes neural networks. The neural

network is a set of processing elements - neurons, interconnected by synapses, which convert the set of input values into a set of desired output values [5-6]. Neural networks are used in a wide range of applications: pattern recognition, control theory, cryptography, data compression. Neural networks have the ability to learn from the sample and generalize with noisy and incomplete data. In the learning process, adjustment of the coefficients associated with synaptic weights is performed.

There are several methods for training neural networks. One of the most well-known and most widely used learning algorithms for multilayer neural networks is the direct dissemination of the method of reverse error propagation [7-8]. This algorithm uses a gradient descent with minimization of the mean square error for each iteration of its execution.

One of the important advantages of neural networks is their ability to take into account the characteristics of attacks, identifying elements that are not similar to those studied [9-10].

3. Method

Neural networks are one of the areas of research in the field of artificial intelligence, based on attempts to recreate the human nervous system, namely the ability of the nervous system to learn and correct mistakes that should enable the work of the human brain to be simulated, albeit roughly, [11]. The neural network consists of neurons. The block diagram of the neuron is shown in Figure 1.

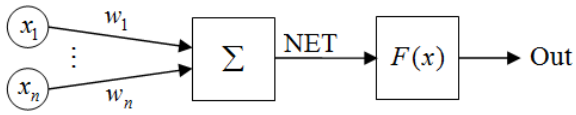

Figure 1: Structural scheme of the neuron

The structure of the neuron from the following blocks represented:

1. Input signals.
2. Weighting factors.
3. Composer and its output NET.
4. The activation function of the neuron F(x).
5. Output signal.

There are many properties in the neural network, but the most important is its ability to learn. The process of training the network reduced to the change in weight coefficients.

$$NET = \sum_n x_n w_n \quad (1)$$

The multilayer neural network includes input, output and hidden layers (Figure 2).

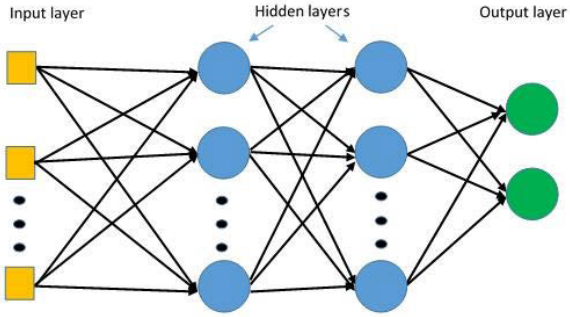

Figure 2: Multilayer Neural Network

Input layer - serves to distribute data over the network and does not do any calculations. Outputs of this layer transmit signals to the inputs of the next layer (hidden or output).

Hidden layers are layers of normal neurons that process data obtained from the previous layer and transmit signals from the input to the output. Their input is the output of the previous layer, and the output is the input of the next layer.

Output layer - usually contains one neuron (maybe more), which gives the result of calculations of the entire neural network. [11].

To conduct research, it was decided to use the NSL-KDD attack database. This database is based on the basis of the KDD-99 on the initiative of the American Association for Advanced Defense Research DARPA. [12]

It covers a wide range of different intrusions. Data is a text file. This file contained both normal vectors and an abnormal activity vector. Abnormal activity is marked by an attack type. All attacks in NSL-KDD are divided into four groups: DoS (Denial of Service Attack), U2R (Users to Root Attack), R2L (Remote to Local Attack) and Probe (Probing Attack). Table 1 lists the types of attacks, their number and the class to which the attack belongs.

Table 1
Information about attacks

Type	Number	Class
back	956	DOS
land	18	DOS
neptune	41214	DOS
pod	201	DOS
smurf	2646	DOS
teardrop	892	DOS

Type	Number	Class
buffer_overflow	130	U2R
loadmodule	72	U2R
perl	34	U2R
rootkit	30	U2R
ftp_write	43	R2L
imap	126	R2L
guess_passwd	1231	R2L
multihop	254	R2L
phf	7	R2L
spy	3	R2L
warezclient	890	R2L
warezmaster	205	R2L
ipsweet	3599	Probe
nmap	1493	Probe
portsweep	2931	Probe
satan	3633	Probe
normal	67343	-

Each record has 42 attributes describing different attributes (table 2).

Table 2

List of attributes for each entry

№	Attribute name
1	duration
2	protocol_type
3	service
4	flag
5	src_bytes
6	dst_bytes
7	land
8	wrong_fragment
9	urgent
10	hot
11	num_failed_logins
12	logged_in
13	num_compromised
14	root_shell
15	su_attempted
16	num_root
17	num_file_creations
18	num_shells
19	num_access_files
20	num_outbound_cmds
21	is_host_login
22	is_guest_login
23	count
24	srv_count
25	serror_rate
26	srv_serror_rate
27	rerror_rate
28	srv_rerror_rate
29	same_srv_rate
30	diff_srv_rate
31	srv_diff_host_rate
32	dst_host_count
33	dst_host_srv_count
34	dst_host_same_srv_rate
35	dst_host_diff_srv_rate
36	dst_host_same_src_port_rate
37	dst_host_srv_diff_host_rate
38	dst_host_serror_rate
39	dst_host_srv_serror_rate
40	dst_host_rerror_rate
41	dst_host_srv_rerror_rate
42	attack_type

The Deductor Academic 5.3 software to construct and test the neural network was used. Deductor is a platform for creating complete analytical solutions. The platform employs advanced methods for extracting, rendering data and analyzing data. Deductor Academic - The free version for educational purposes only intended.

In this paper, the study for attacks like DoS conducted. Therefore, a parser written to extract the necessary vectors. There were 4 files for training and testing of the neural network: KDDTrainDos + .txt, KDDTestDefinedDos + .txt, KDDTestNormalDos + .txt, KDDTestUndefinedDos + .txt. The files contain a set of training data, a set of known attacks and normal vectors that listed in the training set, as well as a set of unknown attacks.

The file for training the neural network contains 7,000 records, the contents of the file given in Table 3.

Table 3

Contents of the training file

Attack name	Number of attacks
back	556
neptune	4000
smurf	1446
teardrop	492
normal	506

A test file with known attack types contains 5000 entries. The table of contents given in Table 4.

Table 4
The contents of the file for testing with known types of attacks

Attack name	Number of attacks
back	400
neptune	3000
smurf	1200
teardrop	400

A normal testing file contains 781 entries. The file with unknown types of attacks are attacks such land and pod, the number of entries is 219. Research of intrusion detection was performed using multilayer perceptron.

4. Experimental results

Before the construction of the neural network training data set excluded parameters have the same meaning throughout the sample. This was done to accelerate results.

The first neural network was built on 28 parameters. It consisted of an input, one hidden and output layers. The input and hidden layer neurons had 28 each, consisting of one output neuron containing conclude attack (1 - attack, 0 - normal traffic). This neural network is presented in Figure 3.

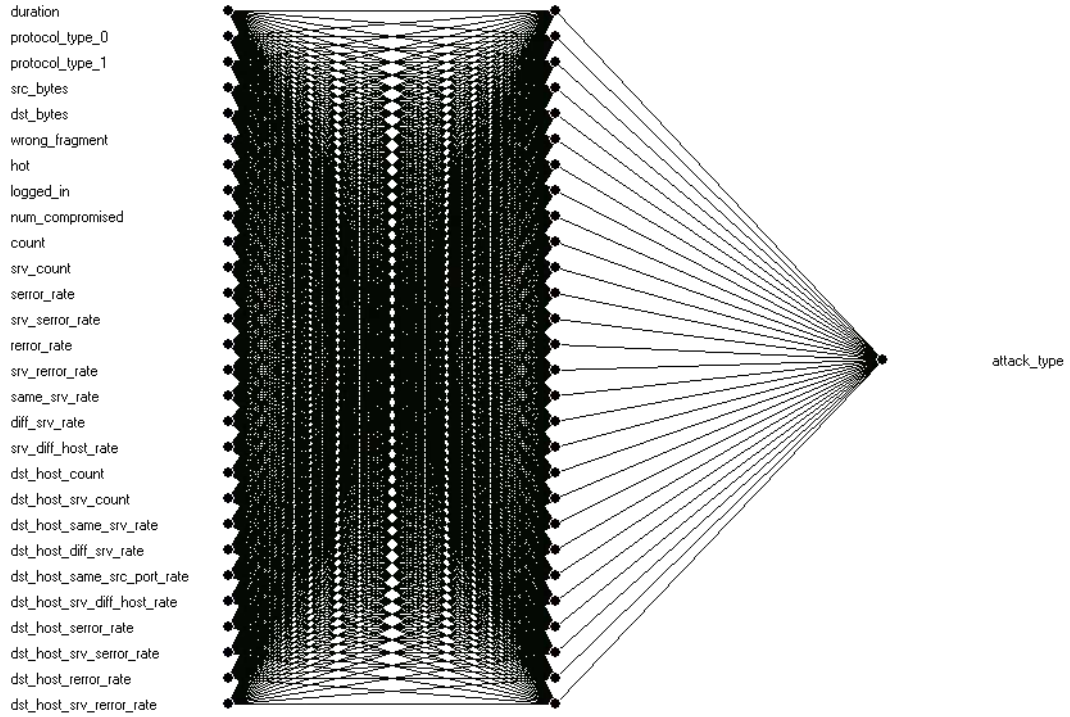

Figure 3: Neural network 28x28x1

After building a neural network was conducted three tests to assess the quality of its work in detecting attacks. The first test was carried out for attacks from known types for neural network (back, neptune, smurf, teardrop). Neural network with almost 100% (99.78%) accurately recognizes known types of attacks. Further testing was conducted for normal traffic. In this case, the results were similar to results for known types of attacks (98.98%). And the last test was performed with unknown types of attacks for the neural network, namely attacks like land and pod.

Unlike previous tests, the result is very different. That is, in this case, we can say that only every 4th attack will be detected. But it should be noted that since these types of attacks were not present in the training set, we can say that this is a good result. And also the knowledge that such methods as statistical analysis and the method of signature analysis, in the absence of information about the attack data in general, would mark them as normal traffic suggests that the use of neural networks to detect intrusions is justified, since they have the ability to adapt to unknown attacks.

Since satisfactory results were obtained, a decision was made to construct neural networks with different parameters to determine the optimal configuration for detecting the maximum number of attacks. Changes were made in the number of input parameters, in the change of activation

function and its steepness, and in the number of hidden layers.

The following neural networks have a common configuration: 15 input neurons, 16 neurons in the hidden layer and 1 output neuron (Figure 4).

All neural networks 15x16x1 have the same look, the difference between them is only in different activation functions and the value of the slope parameter (Table 5).

Table 5
Test Neural Networks

№	Size	Activation function	Slope function
1	15x16x1	Sigmoid	1
2	15x16x1	Sigmoid	1,5
3	15x16x1	Hypertangens	1
4	15x16x1	Arctangens	1

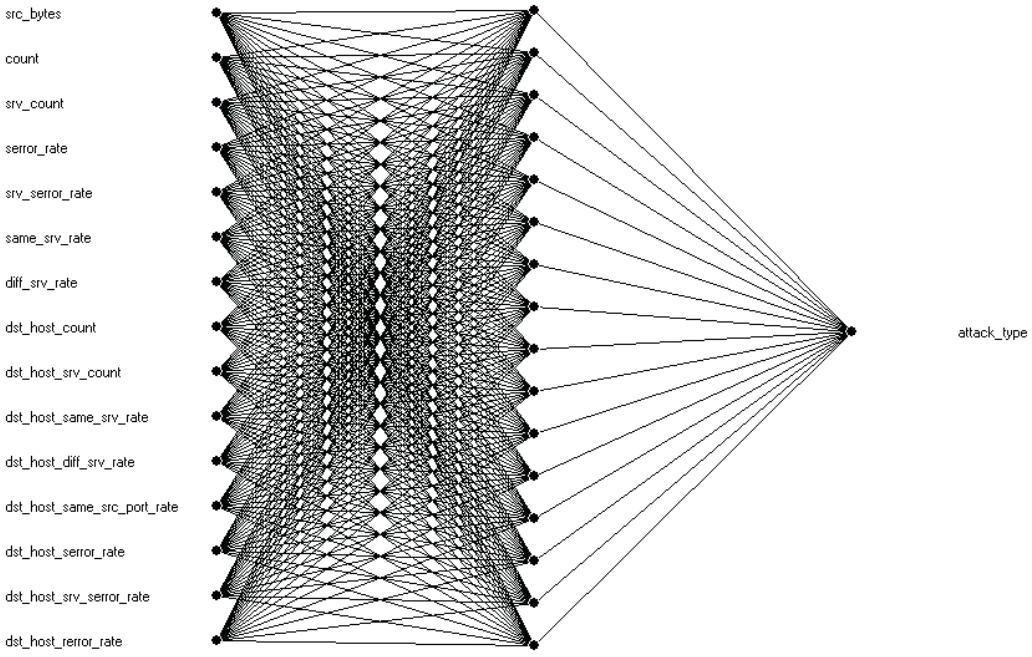

Figure 4: Neural network 15x16x1

For each of the networks built previously described tests were conducted, such as intrusion detection with known types, normal traffic and attacks with unknown types. The results obtained with the use of these neural networks are presented in Table 6.

Table 6
Results of neural network 15x16x1

№	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
1	99,76	97,18	34,25
2	99,88	95,13	33,79
3	100	0	100
4	99,18	60,69	57,08

Based on the results, we can say that the best of all has shown itself the function of activation of the sigmoid. The artagens and the hypertension, however, did not give satisfactory results, although the recognition of attacks with an unknown type has increased significantly, the quality of the definition of normal traffic has suffered greatly. Therefore, in this case, we can conclude that for this task, the function of activating the sigmoid is better suited. Regarding the slope coefficient, we can say that the coefficient 1.5 did not improve the results. Therefore, the following studies were conducted with sigmoid and factor 1, since the best results were obtained for this configuration. Further changes relate only to the number of neurons and the number of hidden layers.

Next, neuronal networks with 21, 26 and 31 neurons were constructed on a hidden layer.

Further tests were carried out. The results are presented in Table 7.

Table 7
Results of neural networks

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
15x21x1	99,68	95,77	33,79
15x26x1	99,78	96,03	33,79
15x31x1	99,7	96,8	34,7

The last two experiments were conducted with a neural network with two hidden layers (Figure 5) and a neural network with a smaller number of input neurons - 10 (Figure 6).

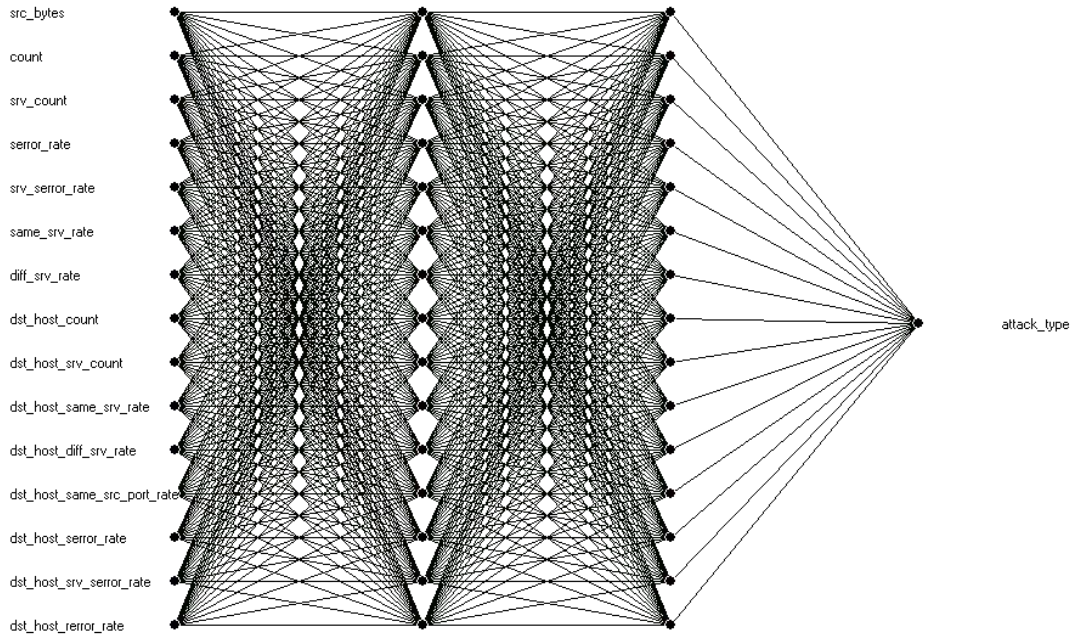

Figure 5: Neural network with two hidden layers

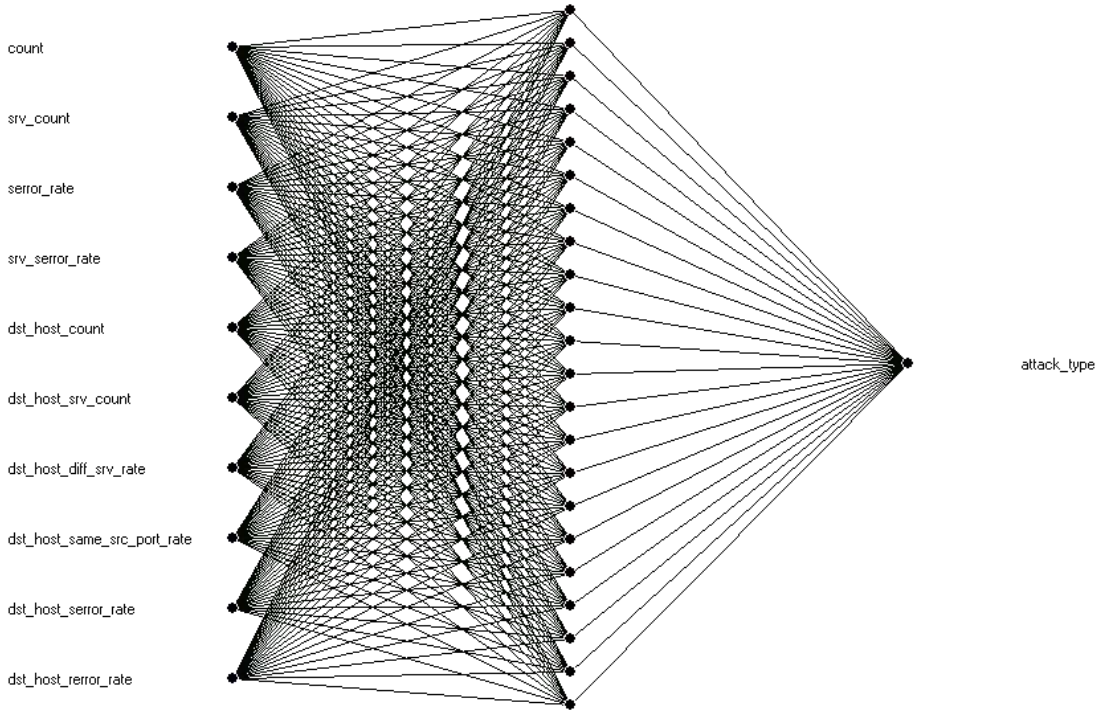

Figure 6: Neural network with 10 input neurons

The results represented in Table 8.

Table 8
Results of neural networks 15x15x15x1 and 10x22x1

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
15x15x15x1	99,8	95,01	34,25
10x22x1	99,96	93,34	31,51

From the results it can be seen that the neural network with 10 input neurons has worse results than neural networks with more input parameters. Thus, a strong reduction in the number of input parameters has a negative effect on the result. As for a neural network with two hidden layers, it has approximately the same results as the neural networks 15x16x1 and 15x31x1. If you summarize the value (to sum up the percentage and find it divided by the number of experimentation findings) for networks with better results, namely for 15x16x1, 15x31x1 and 15x15x15x1, then you can see which neural network has better coped with the task (table 9).

Table 9
Neural network results with the best results

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%	Generalized value, %
15x15x15x1	99,8	95,01	34,25	76,35
15x31x1	99,7	96,8	34,7	77,07
15x16x1	99,76	97,18	34,25	77,06

5. Conclusions

Among the considered neural networks, the best with the task of detecting attacks was copied neural network with 31 neurons in the hidden layer.

So, as can be seen in comparison with the first experiment, where the percentage of unknown attacks was 27.4% managed to get an increase to 34%, that is, every third unknown attack would be detected.

Thus, we can conclude that although the percentage is not very large, it is satisfactory, as it is much better than skipping attacks as normal traffic. It can be said that the use of multilayer perceptron for this task is justified.

6. References

[1] Beqiri E. Neural Networks for Intrusion Detection Systems. In: Jahankhani H., Hessami A.G., Hsu F. (eds) Global Security, Safety, and Sustainability. ICGS3 2009. Communications in Computer and Information Science, vol 45. Springer, Berlin, Heidelberg

[2] Reddy E. K. Neural networks for intrusion detection and its applications //Proceedings of the World Congress on Engineering. – 2013. – Т. 2. – №. 5. – С. 3-5.

[3] Mustafaev, AG, A Neural Network System for Detecting Computer Attacks Based on Analysis of Network Traffic, Security Issues. - 2016. - №. 2. - p. 1-7.

[4] Alekseev A.S., TEACHING THE APPLICATION OF NEURAL NETWORKS FOR DISPLACEMENT OF INCORPORTS // Problems of modern pedagogical education. - 2017. - no. 57-6. - p. 44-50.

[5] Subba B., Biswas S., Karmakar S. A neural network based system for intrusion detection and attack classification //2016 Twenty Second National Conference on Communication (NCC). – IEEE, 2016. – С. 1-6.

[6] Park S., Park H. ANN Based Intrusion Detection Model //Workshops of the International Conference on Advanced Information Networking and Applications. – Springer, Cham, 2019. – С. 433-437.

[7] E. Belov, M. Maslennikov, A. Korobeinikov. The use of a neural network to detect network attacks. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. - 2007. - №. 40

[8] Subba B., Biswas S., Karmakar S. Intrusion detection systems using linear discriminant analysis and logistic regression //2015 Annual IEEE India Conference (INDICON). – IEEE, 2015. – С. 1-6.

[9] Fernandes G. et al. A comprehensive survey on network anomaly detection //Telecommunication Systems. – 2019. – Т. 70. – №. 3. – С. 447-489.

[10] Kaja N., Shaout A., Ma D. A two stage intrusion detection intelligent system //The international arab conference on information technology, IEEE-ACIT. – 2017.

[11] NSL-KDD dataset // https://github.com/defcom17/NSL_KDD