КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1(17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.4656
UDC 004.03

Ilyenko Anna
Candidate of Technical Sciences, assistant professor , assistant professor of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ilyenko Sergii
Candidate of Technical Sciences, assistant professor , assistant professor of Automation and Energy Management Department National Aviation University of Kyiv, Aerospace Faculty, Ukraine
ORCID ID: 0000-0002-0437-0995
ilyenko.s.s@nau.edu.ua

Kravchuk Iryna
Assistant of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
iryna.kravchuk@npp.nau.edu.ua

Herasymenko Marharyta
Student Information Security Systems Department
National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID ID: 0000-0003-1142-0572
margaret75gerald@gmail.com

PROSPECTIVE DIRECTIONS OF TRAFFIC ANALYSIS AND INTRUSION DETECTION BASED ON NEURAL NETWORKS

Abstract. The main problems of the network security at the moment are the difficulty of combining existing systems from different vendors and ensuring their stable interaction with each other. Intrusion detection is one of the main tasks of a proper level of network security, because it is they who notify about attacks and can block them when detected. Today, monitoring and analyzing the quality of traffic in the network, detecting and preventing intrusions is helped by IDS systems and IDS systems of the new generation IPS. However, they have been found to have certain drawbacks, such as the limitations of signature-based systems, as static attack signatures limit the flexibility of systems and pose the threat of missing detection of other attacks not entered into the database. This gives rise to the creation of more and more new hybrid systems, but the challenge is to ensure their efficiency and flexibility, which is helped by the use of artificial neural networks (ANNs). This paper considers ways to improve the use of the convolutional neural network model itself by means of modified processing, data analysis, the use of Softmax and FocalLoss functions to avoid the problem of uneven distribution of sample data by the ratio of positive and negative samples, based on training using the KDD99 dataset. The article provides practical examples of possible integration of IDS and ANN systems. Combinations of backpropagation neural networks and radiant-basis neural networks, which showed some of the best results and proved that the combination of networks helps to increase the efficiency of these systems and create a flexible network adjusted to the needs and requirements of the systems. Although the use of artificial neural networks is a popular tool, it has identified a number of disadvantages: critical dependence on the quality of the dataset, which pours both the quality of networking and the amount of data (the more data, the better and more accurate the network training). But if the data is excessive, there is a chance of missing such implicit, but also dangerous attacks as R2L and U2R.

Key words: neural networks, intrusion detection systems, KDD99, convolutional neural network.

ISSN 2663 - 4023

INTRODUCTION

Formulation of the problem. In today's world, security is a critical issue. Networks already have a long history, in them for some reasons, depending on the needs and capabilities of organizations, there are still architectures in which new ones are built on top of outdated system components. This creates more and more threats in addition to the emerging vulnerabilities of negative integration of new elements and sometimes their inability to interact with each other, device identification problems, the rapid development of cloud technologies, an increase in the number of physical devices and connectors, the spread of SaaS platforms, which motivates cyber security specialists to find new security and auditing methods, ensuring reliable, fast and most importantly secure connections from anywhere, integrity, availability and, of course, privacy, including prevention of possible legal and financial consequences in the form of fines for compromise.

Attacks can occur at different levels, so network security requires three areas of control:

- Physical. Direct restriction of unauthorized access to system elements.
- Technical. Protection of data stored on the network. For example, using servers or installing devices that perform certain security functions in the network environment, outside or in the path of network traffic, which allows you to discard potentially dangerous data packets, detect malicious information and eliminate threats.
- Administrative. Limiting access based on defining the rights and roles of interacting with the system.

Most traditional security tools are designed to protect one intended segment of the network, they are not integrated into the network and cannot interact with each other. However, security systems can struggle to keep up when the network is constantly changing – optimizing connections, redirecting workflows, adding new boundaries or endpoints, or scaling to meet changing requirements. Therefore, in order to determine network protection methods, it is necessary to correctly assess all possible risks, weaknesses, to take the right measures, to ensure backup in case of physical damage to hardware or unexpected failures during downtime, and when changing the structure of the system, to conduct a second review of all available means. Especially when using remote devices, it is necessary to take additional measures of traffic analysis in order to detect intrusions in time or to prevent their occurrence. It's the only way to maintain visibility, centralize control, and implement AI-powered services to automatically detect and respond to threats.

Analysis of recent researches and publications. Today, monitoring and analyzing the quality of traffic in the network, detecting and preventing intrusions is helped by IDS systems and IDS systems of the new generation IPS [1, 5, 7]. However, they have been found to have certain drawbacks, such as the limitations of signature-based systems, as static attack signatures limit the flexibility of systems and pose the threat of missing detection of other attacks not entered into the database. Also, systems based on the detection of anomalies have a probability of false activation, which only adds to the work of specialists.

Network security works to protect data on the network from a security breach that could lead to data loss or unauthorized use and even destruction. There are a variety of threats that can potentially harm a network, each targeting all elements of a system. Today, there is a wide range of tools that can provide comprehensive network security: Metasploit, which allows you to scan and evaluate system security; Nessus to identify and fix vulnerabilities, bugs and errors in applications, operating systems and devices; Argus, which helps to provide any analysis of the entire network and its traffic; Wireshark detects the nature of the interaction between devices; Aircrack, which provides a suite of Wi-Fi security tools.

ISSN 2663 - 4023

The purpose of the article. The main problems at the moment are the difficulty of combining existing systems from different vendors and ensuring their stable interaction with each other, and the problem of surface connection of elements, which results in the complexity of system scalability, which does not help to adequately identify malicious changes that can be used or directly created by an attacker.

Therefore, protection with "inbound" components such as firewalls, anti-virus programs, and virtual private networks (VPNs) for working from remote locations and beyond, which help protect the network from attacks by controlling, identifying, and analyzing traffic, should be important and a priority. And the first means of traffic control, which still remains the most effective, is the introduction of intrusion detection systems (IDS) and the new generation of IDS systems - intrusion prevention systems (IPS). Intrusion detection is one of the main tasks of a proper level of network security, because it is they who notify about attacks and can block them when detected.

This gives reasons to the creation of more and more new hybrid systems [2, 3, 10-12], but the challenge is to ensure their efficiency and flexibility, which is helped by the use of artificial neural networks (ANNs). This allows professionals to improve information gathering methods, identify security risks, and quickly respond to emerging threats before an attacker takes advantage of them. In this work, the current state of network traffic security, existing threats and vulnerabilities, and the possibilities of using a combination of IDS or IPS systems with ANNs with various architectures, training methods and datasets will be discussed in detail.

THEORETICAL BASICS OF RESEARCH

At the beginning of integration in IPS or IDS systems, these tasks were performed by ML algorithms, but they caused many false positives, which added work to specialists. Algorithms based on deep learning, unlike typical ML algorithms, deal with large data sets with different attributes (input data). Therefore, ML has completely replaced deep learning, convolutional neural networks, and recurrent neural networks (RNNs), which have enabled traffic analysis with better accuracy. In addition, the flexibility of use consists in the adaptation of their training: with a teacher (compared to the target result) and without a teacher (without a defined result).

A convolutional neural network (CNN) can automatically learn the characteristics of data. The proposed architecture of such a network (Fig. 1, 2) [8, 9], for example, is able to process a large amount of data on computing resources and increase the basic processing efficiency by reducing the load on the network bandwidth.

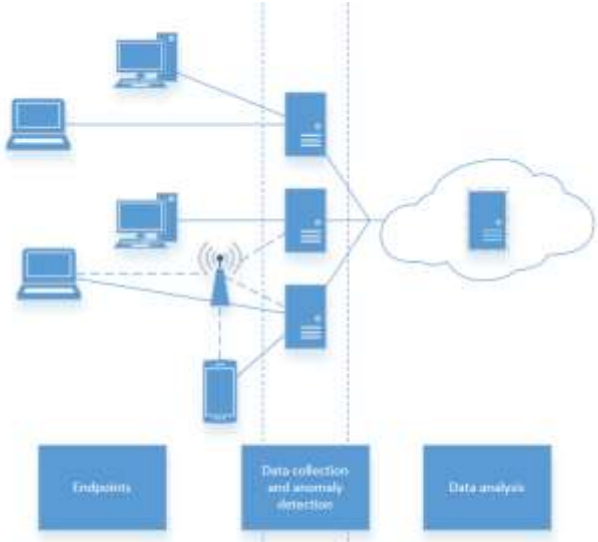

Fig. 1. Network architecture

ISSN 2663 - 4023

Training of such a network takes place according to the following algorithm:

1. Initialization of weights with random parameters.
2. Creation of the educational sample.
3. Comparison of the network output with the desired output. Error calculation.
4. Determination of the scaling factor of the value of each neuron.
5. Setting weights coefficients: $w_N = w_N + \Delta w_N$, where w_N is a calculated value using the delta rule.
6. Repeating the process on neurons of the previous level.

The idea is to improve the use of the convolutional neural network model itself by means of modified processing, data analysis, the use of the Softmax function and FocalLoss to avoid the problem of uneven distribution of sample data by the ratio of positive and negative samples. In this example, the experiment is performed using KDD99, offline network data in a data set, in a CSV file, which contains a five million data set of malicious or benign network traffic and network behavior, which is defined by the [3, 4] attack labels (range of values and classification of the attack type is shown in Table 1), for example U2R and R2L are hidden in the download of data packets. The probability distribution of the data for each attack type is uneven. Denial of Service, Probe, User to Root, and Remote to Local are the four attack data categories in KDD. For training a network, the quality of the training data is critical, so in order to obtain the most accurate results, it is necessary to perform pre-processing on the data, which can be divided into data set cleaning, type conversion to integer or binary data types, alignment, normalization of sample attributes to filter redundant data and remove redundant data. duplicate entries.

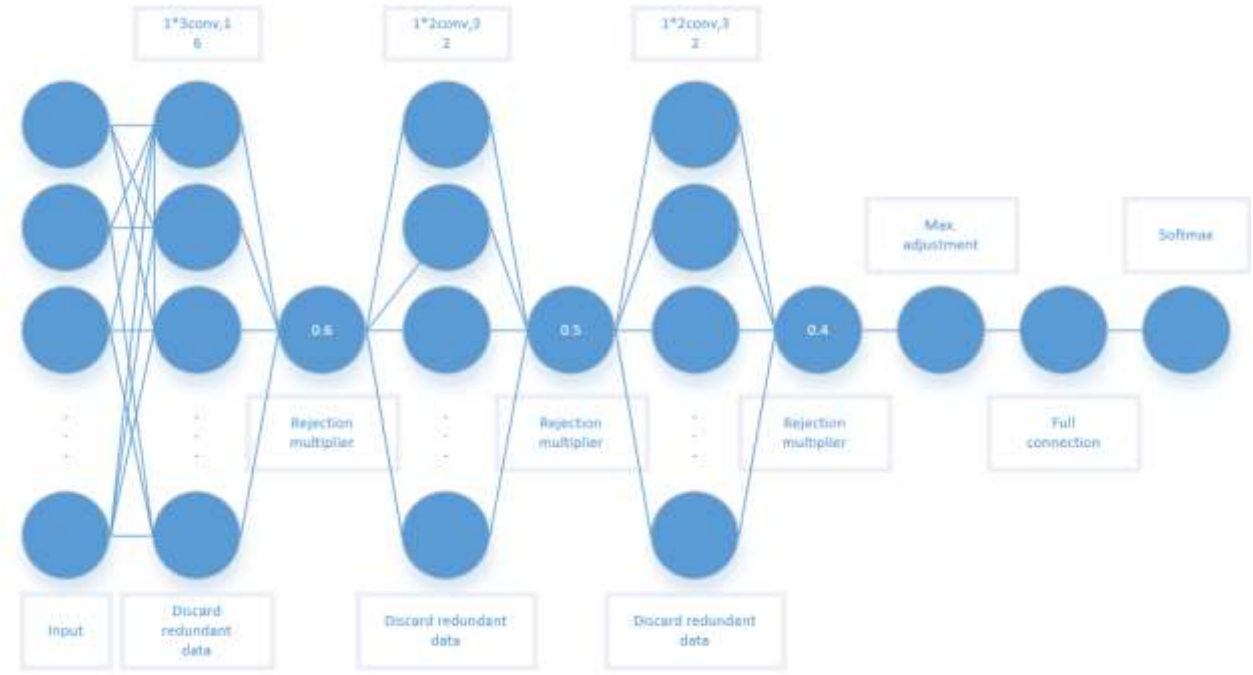

Fig. 2. Neural Network architecture

ISSN 2663 - 4023

Table 1.1

Results of values α and τ

α	τ	Accurancy, %	Detection,%	False activation, %
0	0.6	97.32	94.71	0.73
1	0.4	98.68	96.69	0.64
2	0.2	98.44	97.24	0.33
5	0.2	97.57	96.15	1.07

The method for normalizing sample attributes is as follows: let there be a certain sequence of data $x = \{x_1, x_2, \ldots, x_n\}$, which has a minimum and maximum value x_{min} and x_{max}, respectively. Suppose that x_i is a normalized value, then:

$$x_i = \frac{x_i - x_{max}}{x_{max} - x_{min}}, x[x_{min}, x_{max}], i \in [1, n], \quad (1)$$

The range of values of x_i lies between 0 and 1.

The created CNN model for use in the intrusion detection system is shown in Fig. 2. The network has 10 layers: 1 input layer, 3 convolution layers, 3 extraction layers, 1 max pooling layer, 1 fully connected layer, and 1 output layer. After their preliminary processing, layers 2, 4 and 6 are directly convolution layers. In the output layer, classification takes place directly using the Softmax function, which is a generalization of the logistic regression model for multiclassification in CNN. In the multiclassification problem, the class label y takes $k(k > 2)$ The created CNN model for use in the intrusion detection system is shown in Fig. The network has 10 layers: 1 input layer, 3 convolution layers, 3 extraction layers, 1 max pooling layer, 1 fully connected layer, and 1 output layer. After their preliminary processing, layers 2, 4 and 6 are directly convolution layers. In the output layer, classification takes place directly using the Softmax function, which is a generalization of the logistic regression model for multiclassification in CNN. In the multiclassification problem, the class label y takes $(x_1, y_2), (x_2, y_2), \ldots, (x_n, y_n), y_i$, which lies on the interval $\{1,2,\ldots,k\}$. The function guess (2) and classify (3) can be defined as follows:

$$g_\vartheta(x^{(i)}) = \begin{bmatrix} p(y^{(i)} = 1 | x^{(i)}; \vartheta) \\ p(y^{(i)} = 2 | x^{(i)}; \vartheta) \\ \vdots \\ p(y^{(i)} = k | x^{(i)}; \vartheta) \end{bmatrix} = z * \begin{bmatrix} e_1{}^{\vartheta} x^{(i)} \\ e_2{}^{\vartheta} x^{(i)} \\ \vdots \\ e_k{}^{\vartheta} x^{(i)} \end{bmatrix}, z = \frac{1}{\sum_{j=1}^{k} e^{\vartheta_j{}^k x^{(i)}}}, \quad (2)$$

where $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$ are model parameters, z represents the normalization of the probability distribution.

$$J(\vartheta) = -\frac{1}{m}\left[\sum_{i=1}^{m}\sum_{j=1}^{k} 1\{y^{(i)} = j\} \log \frac{e^{\vartheta_j{}^T x^{(i)}}}{\sum_{j=1}^{k} e^{\vartheta_j{}^T x^{(i)}}}\right], \quad (3)$$

Ймовірність класифікації x into category j in Softmax:

$$p(y^{(i)} = j | x^{(i)}; \vartheta) = \frac{e^{\vartheta_j{}^T x^{(i)}}}{\sum_{j=1}^{k} e^{\vartheta_j{}^T x^{(i)}}}, \quad (4)$$

Although the use of ANNs is a popular tool, a number of shortcomings were identified in it: critical dependence on the quality of the dataset, which affects the quality of network

training, and on the amount of data (the more data, the better and more accurate the network training). However, if there is too much data, there is a chance to miss such implicit, but nevertheless dangerous attacks, such as R2L and U2R.

Usually, in the CNN architecture, each parameter in the matrix affects the interaction between the input and output layers, but the basis of this Gated Convolutional Neural Network (GCNN) implementation is discarding redundant information and keeping the desired one (dropout operation), since the CNN model is prone to creating redundant data, which has a great impact on the effectiveness of the actual classification. Some features are necessary to solve a particular categorization task, while others are unnecessary and redundant. In addition, datasets with a large number of feature vectors are difficult to train and test. Therefore, the convolution formula can be presented:

$$A = E * \omega_1 + b_1,$$
$$B = E * \omega_2 + b_2,$$
$$h_1(E) = A * ReLu(B), \quad (5)$$

where E is the result of the output layer, ω_1 and ω_2 are weight matrices, b_1 and b_2 are offsetsя, $ReLu$ is an activation function.

Another example of the use of networks is a multilayer forward propagation network or self-organizing Konochen maps in IDS [6]. The creation of this model is motivated by the fact that some IDS developers use ANNs as a pattern recognition technique that helps optimize the result obtained at the network output. The advantage of a multilayer direct propagation network (Fig. 3) is the minimization of the loss function (quadratic error function). The basis is the formation of the basis of the training set and the change of weights during training (usually, with the help of the backpropagation algorithm) in such a way that the output corresponds to the training data sample as much as possible. Konochen self-organizing maps are a good example of cluster analysis with unsupervised learning. In this architecture, there is a certain initial set of data, the weight values are random at the beginning and are updated only for active output neurons based on Kohonen's rule.

An example of the use of ANNs is also their use in IDS systems based on the detection of access abuse [29]. This method consists in the signature determination of attacks and the formation of a database.

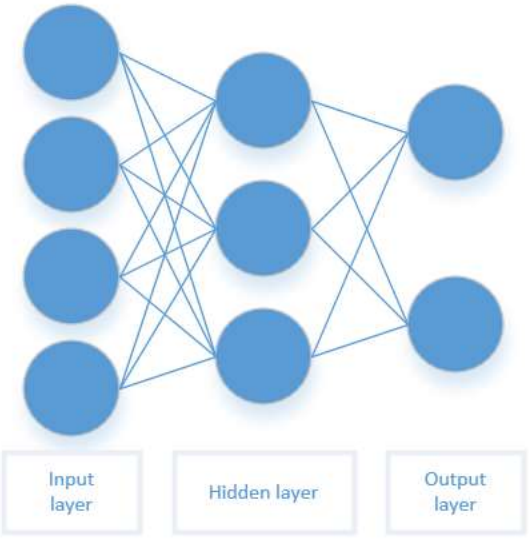

Fig. 3. Architecture of a multilayer forward propagation network

ISSN 2663 - 4023

An attack can only be detected in the active phase, when it is causing or has already caused damage, so for example in port scanning it is difficult for IDS systems to identify it as an intrusion, as the source address or source port can easily be changed. ANNs with the method of learning without a teacher and back propagation of the error can help in this. Such a system will analyze clusters of incoming packets and build its database, even in the presence of incomplete or inaccurate data. And the advantage, of course, lies in the flexibility and inherent speed of neural networks in predicting events, detecting abuse of access, learning new signs of attacks, setting the probability threshold of a potential threat, etc. But this method of detecting intrusions has certain disadvantages. First, such a network strongly depends on the quality of the data of the methods on the basis of which it is trained, and secondly, it requires a huge amount of data, which is difficult to obtain for privacy reasons.

That is, the given ANN in IDS systems can be attributed to IDS based on the detection of anomalies, since they can determine deviations from the adequate values of the system, but the deficiency lies in the determination of these values. The system must determine this itself and be capable of summarizing all data.

The next example of combining IPS with ANNs is a combination of back-propagation neural network (BPA) and radial basis function (RBF) neural networks based on training on the KDD-99 dataset [4]. Most existing identifiers use all the functions of the network packet to search for known intrusion patterns. A clearly defined feature selection algorithm makes the classification process more efficient.

The main feature of the BPA architecture is to minimize the total error of the network by calculating the error of each input layer neuron and adjusting the weights in the reverse direction. This is quite a complex process, since the hidden nodes are not directly related to the error, but are connected through the nodes of the next level. Thus, starting from the source layer, the error propagates back through the network, layer by layer.

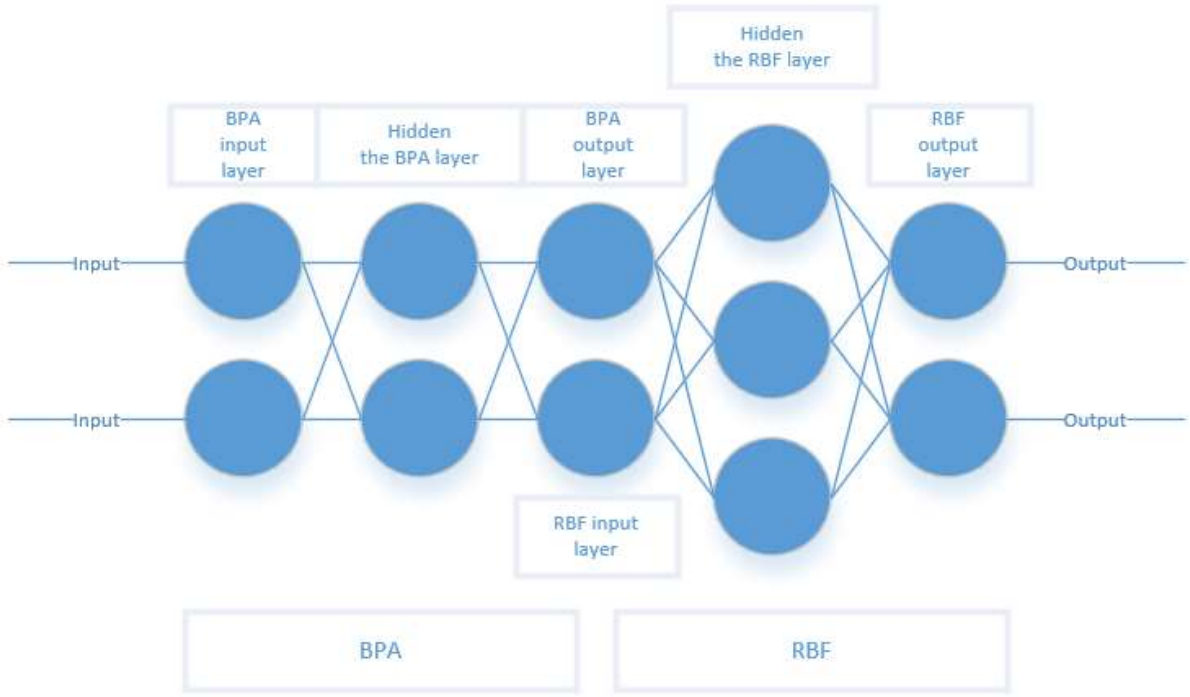

Fig. 4. Architecture of combined BPARBF

The basis of the RBF model is the use of a radial basis function as an activation function. This architecture has input, hidden and output levels. The following parameters are defined for the learning process:

1. The number of neurons in the hidden layer.
2. The radius of each RBF function in each dimension.
3. The center of each hidden layer of the RBF function.
4. Weights applied to the outputs of the RBF function.

The model of the combined BPARBF looks as follows (Fig. 4). The input layer sends data to all hidden nodes where the basis function is calculated. An output layer node summarizes its inputs to produce a network output. Each connection between the hidden and output layers is weighted with an appropriate coefficient.

RESULTS

The test results (table 2) show that the accuracy values are much higher than those of other algorithms. The KDD99 dataset contains five classes of intrusion data types, the detection results of which are shown in the tables.

Table 2

Results of comparing the accuracy of algorithms

Algorithm	Initial	Probe	DoS	U2R	R2L
Proposed algorithm	78.73 %	87.47 %	96.56 %	73.85 %	92.97 %
CNN	72.72 %	75.98 %	93.55 %	71.84 %	92.54 %
Recurrent NN	70.37 %	73.36 %	90.34 %	63.67 %	89.01 %
Kohonen's map	63.51 %	74.57 %	83.47 %	68.73 %	86.76 %

Even the use of ANNs is a popular tool, a number of shortcomings were identified: critical dependence on the quality of the dataset, which affects the quality of network training, and on the amount of data (the more data, the better and more accurate the network training). However, if there is too much data, there is a chance to miss such implicit, but nevertheless dangerous attacks, such as R2L and U2R.

CONCLUSION

The increase in the amount of information and the constant emergence of threats, the need to protect systems and critical data is extremely important. Weak control of privileged access, non-integrated interaction of tools with each other, low fault tolerance and implementation of DDoS attacks, phishing attacks, SQL injections and other vulnerabilities threaten the existence of the entire system. A practical example of the possible integration of IDS and ANN convolution systems using the Softmax and FocalLoss functions is given to avoid the problem of uneven distribution of sample data by the ratio of positive and negative samples. The test results show that the considered means of integration of intrusion detection systems and neural networks is much more accurate than other algorithms.

REFERENCES

1 Cao, Y., Zhang, L., Zhao, X., Jin, K., Chen, Z. (2022). An Intrusion Detection Method for Industrial Control System Based on Machine Learning. *Information*, *13*(7), 322. https://doi.org/10.3390/info13070322.

2 Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., Bahaj, S. A. (2022). Deep learning for intrusion detection and security of internet of things (IOT): Current analysis, challenges, and possible solutions. *Security and Communication Networks*, *2022*, 1–13. https://doi.org/10.1155/2022/4016073.

3 Tian, C., Zhang, F., Li, Z., Wang, R., Huang, X., Xi, L., Zhang, Y. (2022). Intrusion Detection Method Based on Deep Learning. *Wireless Communications and Mobile Computing*, *2022*, 1–8. https://doi.org/10.1155/2022/1338392.

4 Kalpana, Y., Purushothaman, S., Rajeswari, R. (2013). Implementation of intrusion detection using BPARBF neural networks. *International journal of computer science and information security*, *11*(10), 70.

5 Papadogiannaki, E., Tsirantonakis, G., Ioannidis, S. (2022). Network intrusion detection in encrypted traffic.

6 Reddy, K. (2013). Neural networks for intrusion detection and its applications. In *Proceedings of the world congress on engineering*, London (pp. 3–4).

7 Vinchurkar, D., Reshamwala, A. (2022). A review of intrusion detection system using neural network and machine learning technique.

8 Wang, Y., Wang, J., Jin, H. (2022). Network Intrusion Detection Method Based on Improved CNN in Internet of Things Environment. *Mobile Information Systems*, *2022*, 1–10. https://doi.org/10.1155/2022/3850582.

9 Zainel, H., Koçak ,C. (2022). LAN intrusion detection using convolutional neural networks. *Applied sciences*, *12*, 2–4.

10 Zhao, X. (2022). Application of data mining technology in software intrusion detection and information processing.

11 Anna, I., Sergii, I., Marharyta, H. (2021). A Biometric Asymmetric Cryptosystem Software Module Based on Convolutional Neural Networks. International Journal of Computer Network & Information Security, 13(6).

12 Ilyenko, A., Ilyenko, S. (2022). Program Module of Cryptographic Protection Critically Important Information of Civil Aviation Channels. In International Conference on Computer Science, Engineering and Education Applications (pp. 235-247). Springer, Cham.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Ільєнко Анна Вадимівна
Кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет, факультет кібербезпеки комп'ютерної та програмної інженерії, Київ, Україна
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ільєнко Сергій Сергійович
Кандидат технічних наук, доцент, доцент кафедри автоматизації та енергоменеджменту
Національний авіаційний університет, аерокосмічний факультет,
Київ, Україна
ORCID ID: 0000-0002-0437-0995
ilyenko.s.s@nau.edu.ua

Кравчук Ірина Анатоліївна
Асистент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет, факультет кібербезпеки комп'ютерної та програмної інженерії, Київ, Україна
iryna.kravchuk@npp.nau.edu.ua

Герасименко Маргарита Костянтинівна
Магістр, студентка кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет, факультет кібербезпеки комп'ютерної та програмної інженерії, Київ, Україна
ORCID ID: 0000-0003-1142-0572
margaret75gerald@gmail.com

ПЕРСПЕКТИВНІ НАПРЯМКИ АНАЛІЗУ ТРАФІКУ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ НЕЙРОМЕРЕЖ

Анотація. Основними проблемами мережевої безпеки на даний момент є складність поєднання існуючих систем від різних виробників і забезпечення їх стабільної взаємодії між собою. Виявлення вторгнень є одним із головних завдань належного рівня безпеки мережі, оскільки саме вони сповіщають про атаки та можуть блокувати їх при виявленні. Сьогодні контролювати та аналізувати якість трафіку в мережі, виявляти та запобігати вторгненням допомагають системи IDS та системи IDS нового покоління IPS. Однак було встановлено, що вони мають певні недоліки, такі як обмеження систем на основі сигнатур, оскільки статичні сигнатури атак обмежують гнучкість систем і створюють загрозу відсутності виявлення інших атак, не введених у базу даних. Це спонукає до створення все нових і нових гібридних систем, але проблема полягає в тому, щоб забезпечити їх ефективність і гнучкість, чому сприяє використання штучних нейронних мереж. У цій статті розглядаються шляхи вдосконалення використання самої моделі згорткової нейронної мережі за допомогою модифікованої обробки, аналізу даних, використання функцій Softmax і FocalLoss, щоб уникнути проблеми нерівномірного розподілу вибіркових даних за співвідношенням позитивних і негативних вибірок, на основі навчання з використанням набору даних KDD99. У статті наведено практичні приклади можливої інтеграції систем IDS та ANN. Комбінація нейронної мережі зворотного поширення (BPA) і нейронні мережі радіальної базисної функції (RBF), що показали одні з найкращих результатів і довели, що комбінування мереж допомагає підвищити ефективність даних систем та створити гнучку мережу налаштовану під потреби і вимоги систем. Хоча застосування штучних нейронних мереж є популярним засобом, в ньому було виявлено ряд недоліків: критична залежність від якості датасету, яка вливає і на якість навчання мережі, та від кількості даних (чим більше даних, тим краще та точніше походить навчання мережі). Але і з тим, якщо даних буде надмірно, існує ймовірність пропустити такі неявні, але і з тим небезпечні атаки, як R2L and U2R.

Ключові слова: нейронні мережі, системи виявлення вторгнень, KDD99, згорточна нейронна мережа.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Cao, Y., Zhang, L., Zhao, X., Jin, K., Chen, Z. (2022). An Intrusion Detection Method for Industrial Control System Based on Machine Learning. *Information*, *13*(7), 322. https://doi.org/10.3390/info13070322.

2 Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., Bahaj, S. A. (2022). Deep learning for intrusion detection and security of internet of things (IOT): Current analysis, challenges, and possible solutions. *Security and Communication Networks*, *2022*, 1–13. https://doi.org/10.1155/2022/4016073.

3 Tian, C., Zhang, F., Li, Z., Wang, R., Huang, X., Xi, L., Zhang, Y. (2022). Intrusion Detection Method Based on Deep Learning. *Wireless Communications and Mobile Computing*, *2022*, 1–8. https://doi.org/10.1155/2022/1338392.

4 Kalpana, Y., Purushothaman, S., Rajeswari, R. (2013). Implementation of intrusion detection using BPARBF neural networks. *International journal of computer science and information security*, *11*(10), 70.

5 Papadogiannaki, E., Tsirantonakis, G., Ioannidis, S. (2022). Network intrusion detection in encrypted traffic.

6 Reddy, K. (2013). Neural networks for intrusion detection and its applications. In *Proceedings of the world congress on engineering*, London (pp. 3–4).

7 Vinchurkar, D., Reshamwala, A. (2022). A review of intrusion detection system using neural network and machine learning technique.

8 Wang, Y., Wang, J., Jin, H. (2022). Network Intrusion Detection Method Based on Improved CNN in Internet of Things Environment. *Mobile Information Systems*, *2022*, 1–10. https://doi.org/10.1155/2022/3850582.

9 Zainel, H., Koçak ,C. (2022). LAN intrusion detection using convolutional neural networks. *Applied sciences*, *12*, 2–4.

10 Zhao, X. (2022). Application of data mining technology in software intrusion detection and information processing.

11 Anna, I., Sergii, I., Marharyta, H. (2021). A Biometric Asymmetric Cryptosystem Software Module Based on Convolutional Neural Networks. International Journal of Computer Network & Information Security, 13(6).

12 Ilyenko, A., Ilyenko, S. (2022). Program Module of Cryptographic Protection Critically Important Information of Civil Aviation Channels. In International Conference on Computer Science, Engineering and Education Applications (pp. 235-247). Springer, Cham.