до ресурсу: https://blog.appsecco.com/server-side-request-forgery-ssrf-and-aws-ec2-instances-after-instance-meta-data-service-version-38fc1ba1a28a.
[16]. Vakhula, O., Opirskyy, I., Mykhaylova, O. Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach, Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550, (2023) 55-69.
[17]. Kolb, Tobias. (2023). Development and evaluation of a cloud security testing framework for penetration testing and red teaming of AWS cloud environments.
[18]. Dubey, Parul & Tiwari, Arvind & Raja, Rohit. (2023). Introduction To Cloud Computing and AWS. 10.2174/9789815165821123010002.
[19]. Gandhi, Raj & Shahji, Vivek & Kamble, Nitin. (2021). Access Control Model Based on AWS IAM. International Journal of Innovative Research in Computer and Communication Engineering. 9. 14508. 10.15680/IJIRCCE.2021.0911024.
[20]. Dubey, Parul & Tiwari, Arvind & Raja, Rohit. (2023). Cloud Integrations. 10.2174/9789815165821-123010010.
[21]. Dubey, Parul & Tiwari, Arvind & Raja, Rohit. (2023). Identity and Access Management in AWS. 10.2174/9789815165821123010003.

FEATURES OF USING AMAZON INSPECTOR TO IDENTIFY VULNERABILITIES OF CLOUD APPLICATIONS

Vulnerability to various cyber-attacks, loss of data confidentiality, increased number of failures and reduced stability of information infrastructure, increased capital costs, new requirements for data independence, problems with scaling business information infrastructure can be the main problems that a business may face. The above-mentioned problems can serve as a basis for migration to cloud technologies, which in turn will ensure a reduction in expenses for infrastructure support, increase the efficiency of information infrastructure management compared to work in a local environment, and increase the flexibility of the organization. The relevance of the research lies in improving information security, ensuring confidentiality, integrity and availability, identifying application and environment vulnerabilities through the use of built-in AWS services. The purpose of this work is to implement the evaluation and improvement of the security of the working environment and the application deployed on the basis of cloud services by automating the scanning and analysis of the AWS workload.

Keywords: Amazon Web Services, AWS, Amazon Inspector, IAM, cloud technologies, vulnerability, infrastructure, monitoring.

Партика Андрій Ігорович, к.т.н., старший викладач кафедри захисту інформації Національного університету «Львівська політехніка».

Andrii Partyka, Ph.D., Senior Lecturer the Department of Information Security, Lviv Polytechnic National University.
E-mail: andrijp14@gmail.com.
Orcid ID: 0000-0003-3037-8373.

Недодус Богдан Ігорович, студент, спеціальності 125 Кібербезпека Національного університету «Львівська політехніка».

Bohdan Nedodus, student the Department of Information Security, Lviv Polytechnic National University.
E-mail: nedodusbohdan@gmail.com.
Orcid ID: 0009-0007-3822-5829.

DOI: 10.18372/2410-7840.26.18841
УДК 004.77

METHOD OF ANALYSIS OF OUTGOING TRAFFIC PACKAGE SIGNATURES

Nataliia Petliak, Yuliia Khokhlachova

To detect outgoing malicious traffic, a method based on fuzzy logical inference has been developed to analyze signatures of outgoing traffic. The study results indicate that continuing activities in this direction are worthwhile to unload network resources during peak loads. The method verifies the signature of the outgoing traffic packet against a set of rules. The key tasks of the method are connection permission, if the packet signature is defined as permitted during classification; blocking the connection, if it is determined that the signature of the package is prohibited; and adding new signatures to existing dictionaries. During the experiment, the method confirmed its effectiveness. Having a method based on fuzzy logic for signature analysis of outgoing traffic packets has several advantages, including the detection of previously unknown attacks, reduction of the total number of cyber-attacks, prevention of overloading of network equipment, and reduction of the probability of compromise. current network.

***Keywords**: fuzzy logic, signature analysis, outgoing traffic, signature classification.*

RELEVANCE AND PROBLEM STATEMENT

The rapid growth of the number of users of digital technologies leads to an increase in the number of cyber incidents and cyber-attacks on various spheres of activity. Any attack can cause not only significant financial losses but also reputational losses for a certain person, company, or even the state.

Types and methods of attacks change and improve faster than the processes of digitalization of society.

The problem of detecting anomalous traffic does not have a sufficient solution. Well-known intrusion detection systems are focused on detecting attacks on corporate networks, rather than detecting attacks coming from networks, and use their power to attack third parties.

Public computer networks are used mainly in public places. Such an opportunity increases the number of visitors to various institutions at the expense of insignificant material costs. Any person can connect to such a network without identification. This, in turn, allows the offender to additionally hide while performing malicious actions.

Detecting malicious traffic and anomalies plays an important role in security. Therefore, it is necessary to use intrusion detection systems capable of protecting the network from known and future threats.

Existing intrusion detection and prevention systems focus on protecting your network and are not designed to detect anomalous traffic from your network aimed at attacking third parties.

Thus, the main difficulty of detecting malicious and anomalous traffic directly arises from modern trends in the development of information technologies, which are inextricably linked to the constant growth of its parameters: volume; generation speed; the number of traffic sources and recipients; the number of logical flows unrelated to their goals and tasks; increasing the level of data heterogeneity, etc. [1].

All this leads to significant complications for traffic analyzers, since not all existing systems can cope with such large volumes and complexity, and violators hide their actions in the general flow of actions of legitimate users.

Thus, the main contradiction of the subject area is as follows: on the one hand, it is necessary to increase the accuracy of detecting violators, since their actions are constantly improving, and the network traffic of attacks becomes less visible due to the increase in the volume of all traffic in public networks, and the violators themselves mask their actions under legal; on the other hand, existing models, methods and algorithms for detecting malicious and anomalous traffic do not have the necessary efficiency, as they either have a high risk of missing the attacker (type II error) or, on the contrary, the risk of attributing the attacker to a legitimate user (type I error). A possible reason for this contradiction is some subjectivity inherent in all criteria for malicious activity. So, for example, some users identified as violators could simply perform several wrong actions: enter the wrong password, mistakenly upload a document or send a document to the wrong address, connect someone else's device, etc.

The solution to this contradiction may consist in the application of highly effective specialized technologies for processing network traffic in the field of information security, as well as in the combination of existing and new methods of analysis and detection of malicious activity.

Research in this field [2] shows that the search for new solutions, improvement of existing ones, or solutions focused on a narrow problem is being carried out.

In particular, the use of neural networks [3] improves and modernizes existing intrusion detection systems.

In [4], the IPS system only focuses on mitigating DoS attacks by analyzing packets using deep learning techniques.

Anomaly-based IPS using fuzzy logic prevents various distributed denial-of-service attacks [5].

The identification of new signatures in IPS based on SNORT signatures can be solved using decision trees, but the detection of multi-stage attacks requires machine learning techniques, fuzzy logic, and neural networks [6], however, the significant complexity of these systems leads to a significant increase in cost, and it will be impractical for implementation in small and medium networks.

Various methods are proposed in the article [7]; one of the most important methods is intrusion detection systems, which provide quick detection and notification of network intrusions to take prompt action to reduce the amount of damage caused by these attackers. The main problem of the proposed intrusion detection systems is the number of generated false positives and the low percentage of accurate detection of intrusions in them.

The network anomaly detection method proposed in [8] based on fuzzy logic detects DDoS attacks and analyzes their intensity.

A fuzzy network intrusion detection system [9] uses a set of fuzzy rules using symmetric Gaussian membership functions to determine the probability of specific or common network attacks based on packet signatures.

[10] presented methods for monitoring traffic using a fuzzy logic approach that can mitigate attacks and manage resources during their action.

In [11], a fuzzy inference model and system are proposed, and membership functions and fuzzy pro-

duction rules are defined, taking into account the numerous QoS and QoE requirements of multimedia traffic and the state quality of the CS (Current Service) communication channel. The traffic anomaly detection method based on the correlation analysis of the destination IP addresses in the outgoing traffic on the outgoing router [12] is effective, but the proposed approach can only provide anomaly detection near the source, so its use will be impractical in large networks. From the analysis of the subject area and known solutions of network traffic research, it can be concluded that the use of fuzzy logic methods allows to significantly increase the effectiveness of detecting malicious packets, therefore it is considered appropriate to develop a fuzzy logic model and method. A logical conclusion for the signature analysis of outgoing traffic packets, which became the goal of the study.

MAIN PART

The results of studies of computer network (Fig.1) configurations of various sizes indicate the following:

- SOHO networks use routers and switches that can filter IP addresses, MAC addresses, domains, and web content according to certain rules, but do not protect against external or internal malicious actions in the network;

- medium-sized corporate networks use routers and managed switches that allow you to perform a set of measures to protect the network from external attack and may contain basic intrusion detection systems, but do not analyze the traffic that is in the network and do not monitor malicious outgoing traffic;

- large corporate networks use similar network devices, but their difference may be the number of ports and bandwidth, which ensure stable operation for a larger number of users, while parameters related to network security remain unchanged.

After analyzing typical computer network architectures, the following conclusion can be made:

- Wi-Fi access points do not affect network security;

- the equipment used in SOHO networks has no protection or a low level of protection against external attack;

- the equipment used in corporate networks has an average or high level of protection against an external attack or a malicious network user carrying out an attack or unauthorized access in the middle of the network about other network users;

- none of the possible types of equipment analyzes outgoing traffic from the network for its "normality".

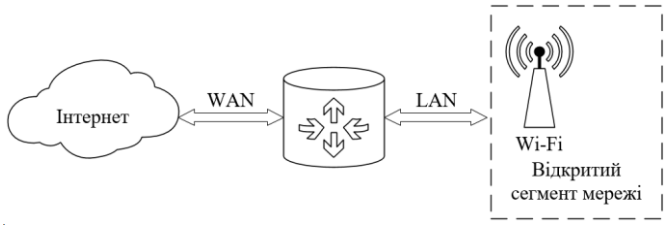

Fig. 1. Typical computer network configuration

In the absence of functionality to detect attacks coming from the network against third parties, the network may experience a decrease in the speed of traffic transmission and compromise of the network.

Based on the identified problem, a fuzzy logical inference model was developed for signature analysis of outgoing traffic packets. This model provides automatic updates of signature dictionaries used to inspect packets of outbound traffic to quickly add previously unknown signatures to dictionaries, including zero-day attacks, by analyzing signatures according to established rules. Analysis of all packet header parameters will slow down the analysis of network traffic and increase the load on network equipment. Therefore, it is advisable to choose parameters that allow identifying the largest number of attacks, to maintain the stable operation of the network (fig.2).

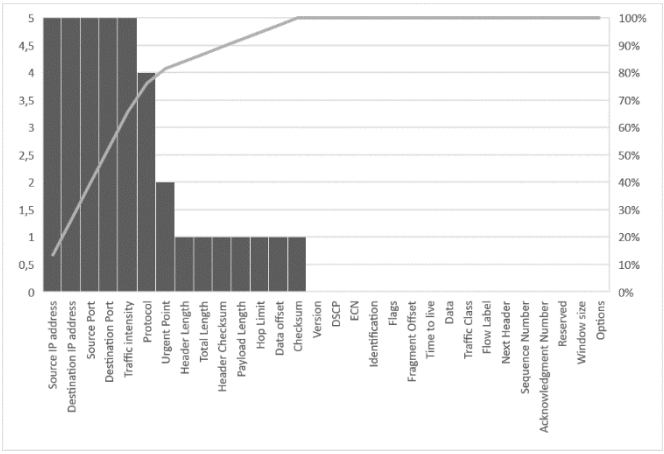

Fig. 2. Using the Pareto principle to optimize parameters for signature formation

It should be noted that the traffic intensity indicator will appear during this analysis. Therefore, the package signature will look like this:

$$s = \{IPs, IPd, Ps, Pd, Pr, Sd, T\}, \qquad (1)$$

where *IPs* is the IP address of the source, is a set of IP address values that can acquire one of three states: prohibition, permission, and unknown; *IPd* is the destination IP address, this is a set of port values that can be in one of three states: deny, allow, and unknown; *Ps* – output port; *Pd* – destination port; *Pr* – the value of the protocol, which can be in one of three states: prohibition, permission, and unknown;

Sd – data transfer rate, *Sd* is a set of data transfer rate values, which can be one of three states: low, medium, and high; *T* – the time of arrival for inspection.

IP addresses are a set of IP address values that combine three sets:

$$IPs = IPsg \cup IPsb \cup IPsn, \quad (2)$$

where *IPsg* – a set of IP addresses defined as allowed; *IPsb* – a set of IP addresses defined as prohibited; *IPsn* – a set of IP addresses that are not defined as allowed or denied.

The elements of the set *IPsg* do not belong to the sets *IPsb* and *IPsn*:

$$IPsg \cap IPsb = \emptyset, \quad (3)$$

$$IPsg \cap IPsn = \emptyset. \quad (4)$$

The elements of the set *IPsb* do not belong to the sets *IPsg* and *IPsn*:

$$IPsb \cap IPsg = \emptyset, \quad (5)$$

$$IPsb \cap IPsn = \emptyset. \quad (6)$$

The elements of the set *IPsn* do not belong to the sets *IPsg* and *IPsb*:

$$IPsn \cap IPsg = \emptyset, \quad (7)$$

$$IPsn \cap IPsb = \emptyset. \quad (8)$$

The sets *IPd*, *Ps*, *Pd, Pr* have a similar content and division of elements.

Packet filtering rules were formed based on the available data.

The rule-based fuzzy logic inference method for outbound traffic packet signature analysis in the previous section performs a real-time comparison of outbound traffic signatures against a set of rules that characterize whether a traffic packet is allowed or denied. category. The main task of the method is:

- allow connections that are considered permitted by the rules;
- prohibit connections that are considered prohibited by the rules;
- adding signatures to the dictionary.

Here is the sequence of the method (fig. 3).

Step 1. Receiving the package.

Step 2. Formation of the package signature.

Step 3. If the generated signature of the packet belongs to one of the rules satisfying the requirement of allowed traffic, then the packet is allowed to be transmitted and proceed to step 4. Otherwise, proceed to step 5.

Step 4. The packet signature is written to the set of allowed connections and the transition to step 8 occurs.

Step 5. If the generated packet signature belongs to one of the rules that satisfy the requirement of prohibited traffic, then the connection in which the packet and the user's IP address are received is blocked, go to step 6. Otherwise, go to step 7.

Step 6. The packet signature is written to the set of forbidden connections and the transition to step 8 occurs.

Step 7: The signature of the packet is written to a set of unspecified connections, after which the packet is allowed to be transmitted.

Step 8. Completion of package processing.

Step 9. If there is a transmission of the following packets, then the transition to step 1 takes place. Otherwise, the transition to standby mode is performed until the next packet is received for verification.

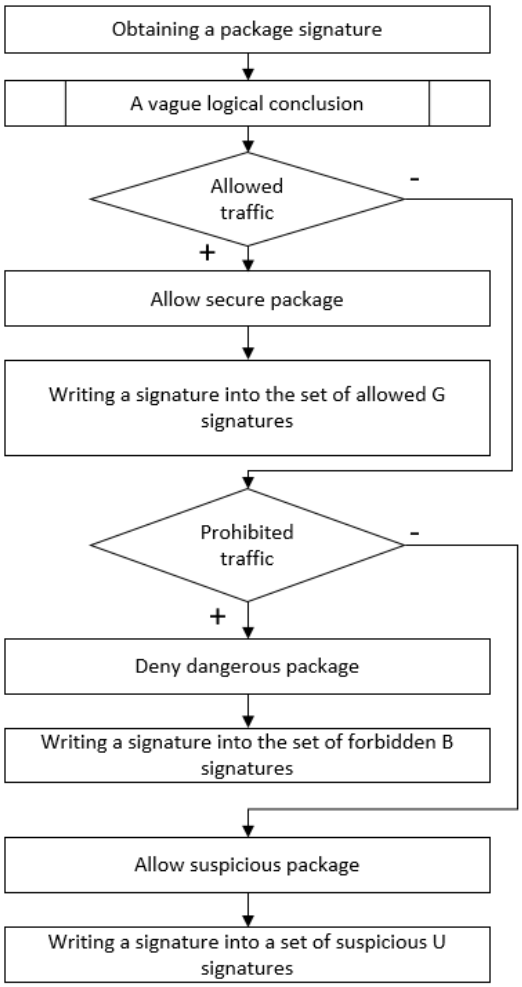

Fig. 3. Graphical representation of the work of the method based on fuzzy logical inference for analyzing the signatures of outgoing traffic packets

The method is implemented using a hardware-software tool, where the software code is developed using fuzzy logic, which checks the output signature (namely, *IPd, Pd, Pr, Sd* elements) for the appropriateness of the traffic type. IP and Ps elements are

used to identify a user on the network. The T element is used to set the timestamp when the signature arrives for verification. After a certain period (the value may vary depending on the average duration of the user's stay on the network), the signature will be deleted. This is necessary so that the size of the dictionary is acceptable. In total, the set contains 81 feature classification rules.

To decide on whether to allow or prohibit sending a packet using a method based on a fuzzy logical conclusion for the signature analysis of outgoing traffic packets, the classification of the signature features of the outgoing traffic packet elements is carried out using Matlab (fig. 4).

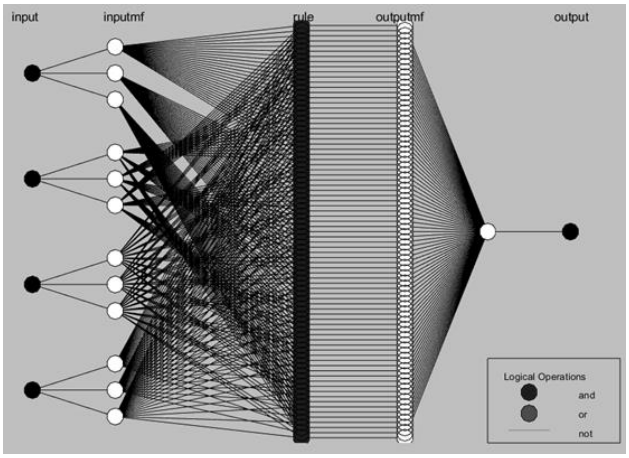

Fig. 4. Scheme of implementation of fuzzy logical conclusion for classification of signs of signature elements using Matlab

Each input and output linguistic variable are defined by a set of terms (fig. 4):

- IPd: prohibition, unknown, permission;
- Sd: low, medium, high;
- Pr: prohibition, unknown, permission;
- Pd: prohibition, unknown, permission.

A trapezoid was chosen as the membership function for inputs and outputs (fig. 5).

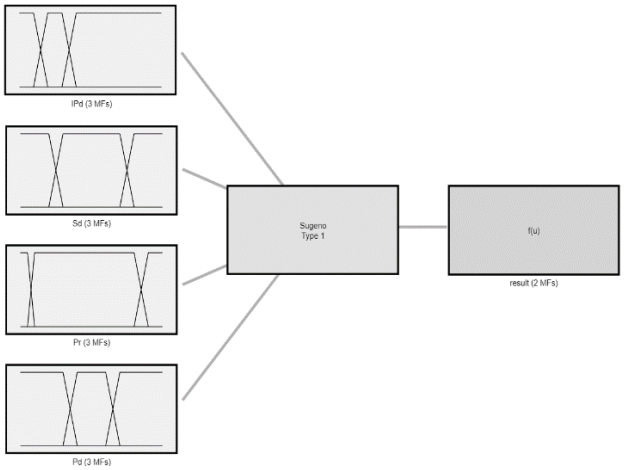

Fig. 5. Sets of terms of input and output variables

The choice is due to the results of network traffic research when the range of values of each parameter can be described by a t-function, which is triangular or trapezoidal (fig. 6), where the upper edge of the trapezoid determines the range of values of each parameter, which allows to assign the analyzed traffic to one or another class (permitted or prohibited). the left and right bounds are deviations that suggest that the traffic belongs to the uncertainty class.

The proposed method is the basis for the implementation of a system for detecting violators in public networks.

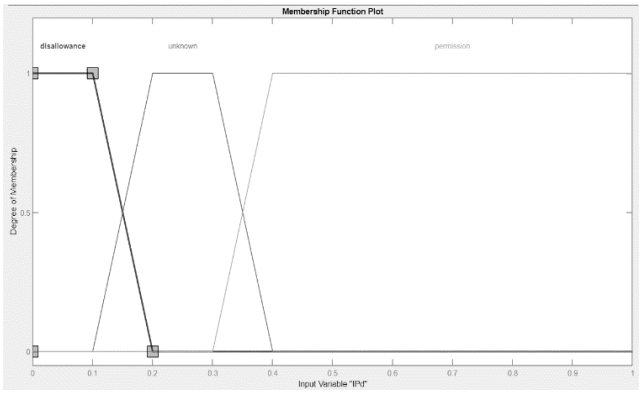

Fig. 6. An example of a membership function

The problem is to ensure the necessary efficiency of the specified system. Therefore, it is necessary to define performance metrics that will allow us to assess how precisely, fully, and qualitatively the developed system fulfills the tasks set before it.

A comparative analysis of research in the field of detection of malicious traffic in public networks made it possible to determine the requirements for an intruder detection system implemented based on the described method. These requirements can be divided into two groups: functional and non-functional. Functional requirements are a list of functions that the system must perform. Non-functional requirements describe the target characteristics of the system, such as time constraints, error rate, completeness, accuracy, etc.

A set of non-functional requirements for a malicious traffic detection system can be defined as three classic components for evaluating efficiency: timeliness (*T*), reasonableness (*O*), and resource intensity (*R*).

Timeliness means the ability of the system to provide a solution to the problem – detection of malicious traffic within the specified period. Requirements for timeliness can be established in a formal form:

$$T \le \min T_s, s \in S, \qquad (9)$$

where T is the time of detection of malicious traffic by the system under development – the time of detection of malicious traffic by system s from the set of all alternative systems S. For the developed system to be used in a mode close to real-time, it must detect malicious traffic in a time that does not exceed a given limit. This timeliness requirement can be established in the following form:

$$P^T(T \le T_{def}) \ge P_0^T, \quad (10)$$

where P^T – the probability of completion of the system process of detecting malicious traffic in the given time, T_{def} – the permissible time of system operation (equal to min T_S), P_0^T – the permissible value of the probability.

Validity refers to the degree to which the system performs the task, namely the proportion of detected intruders compared to their actual presence in the network. The system's formal compliance with this criterion can be determined using a performance metric (which will be discussed later) and presented in a formal form:

a) for completeness, accuracy, neatness, F-measure:

$$\begin{cases} O^i \in O \\ O^i \ge \max O_S^i, s \in S \end{cases}; \quad (11)$$

b) by mistakes:

$$\begin{cases} O^i \in O \\ O^i \min \le O_S^i, s \in S \end{cases}, \quad (12)$$

where O – a set of efficiency metrics, O^i – the efficiency indicator, O_S^i – the efficiency indicator of system s from the set of all alternative systems S.

Increasing the validity of the system's functioning will mean an overall increase in the security of public networks, thus achieving the research objective.

One of the most general indicators characterizing work efficiency is the F-measure, so this requirement can be written as follows: F-measure → max.

Resource intensity characterizes the software and hardware needed by the malicious traffic detection system to solve its task, as well as its characteristics.

Let's define the requirement in a formal form as a set of the following indicators – number of hosts (*h*), average network traffic (*n*), volume of occupied space on SSD/HDD (*v*), average processor load (*c*), average memory load (*m*):

$$\begin{cases} R^i \in R \\ R^i \min \le R_S^i, s \in S \end{cases}, \quad (13)$$

where R – is set of resource intensity indicators, R^i – the resource intensity indicator (*h, n, v, c, m*), and R_S^i – the resource intensity indicator of system *s* from the set of all alternative systems *S*.

The general performance requirements of an evolving malware detection system can be expressed using the following fairly well–known and frequently used performance metrics: TP (True Positive) – the number of packets identified as malicious that are; FP (False Positive) – the number of packets identified as malicious, but they are not; TN (True Negative) number of packets that are not identified as malicious, but are (i.e. not malicious); FN (False Positive) is the number of packets that are not detected as malicious but are not (i.e. malicious). The classic synonym for FP is errors of the first kind, and FN is for errors of the second kind.

The effectiveness of detecting intruders by the system can be evaluated using other metrics that are more understandable for humans: completeness, accuracy, precision, errors, and F-measure.

Completeness (*r*) characterizes the ability of the system to detect violators without taking into account the number of false positives. The completeness rate can be calculated as the proportion of correctly identified malicious sessions among all existing malicious sessions:

$$r = \frac{TP}{TP + FN}. \quad (14)$$

Accuracy (*p*) characterizes the system's ability to detect only intruders without intercepting legitimate traffic. The accuracy rate can be calculated as the proportion of correctly identified malicious sessions among all detected malicious sessions:

$$p = \frac{TP}{TP + FP}. \quad (15)$$

Accuracy (*a*) characterizes the ability of the system to make correct decisions regarding the identification of intruders. The accuracy rate can be calculated as the proportion of correctly identified malicious and benign sessions among all user sessions:

$$a = \frac{TP + TN}{TP + TN + FP + FN}. \quad (16)$$

Error (*e*) characterizes the ability of the system to make incorrect decisions regarding the identification of violators. The error rate can be calculated as the proportion of incorrectly identified malicious and benign sessions among all user sessions:

$$e = \frac{FP + FN}{TP + TN + FP + FN}. \quad (17)$$

The F-measure (*f*) is commonly used to jointly evaluate a system for completeness and precision. The F-measure can be calculated as the ratio of the double product of the completeness and accuracy of the system to their sum:

$$f = \frac{2 * p * r}{p + r}. \quad (18)$$

With the help of the indicated indicators, the developed system of detecting intruders in the public network can be compared both with the closest analogues and with its modifications.

Schematically, the performance indicators TP, TN, FP and TN of the violator detection algorithm can be graphically represented as follows (fig. 7).

To evaluate the effectiveness of this method, a fuzzy logic inference system was developed using Matlab, which was deployed in a test environment. The immediate test environment is a local network in which 50 users, whose activities were not malicious, were working at the same time. Also, 40 attacks of various types and using various devices were carried out on the network (tab. 1). The results of the system are as follows:

Hours of operation are 24 hours

A total of 10,000 packets were analyzed

Including:

- safe packages – 5,000;
- suspicious – 1,000;
- dangerous – 4,000.

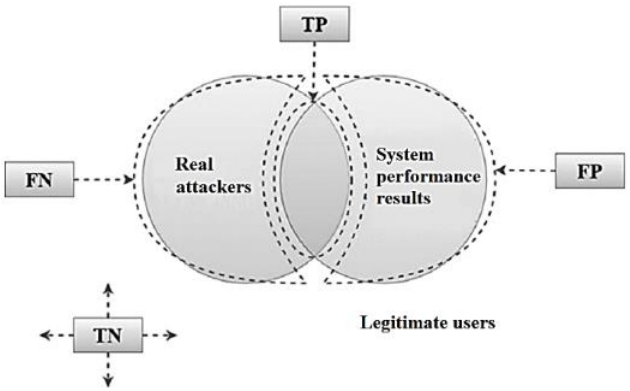

Fig. 7. Graphical interpretation of the efficiency indicators of the violator detection algorithm

Table 1

Data of experimental studies

Packages	Standard	Experiment			
All	10 000	TP	TN	FP	FN
Safe	5 000	4601	-	-	399
Suspicious	1 000	-	536	464	-
Dangerous	4 000	-	4000	-	-

According to the given data, the following efficiency indicators were obtained in percentages:

$$p = 4601/(4601 + 464) * 100\% = 90{,}84\%$$

$$r = 4601/(4601 + 399) * 100\% = 92{,}02\%$$

$$a = (4\,601 + 4\,536)/(10\,000) * 100\% = 91{,}37\%$$

$$e = (464 + 399)/(10\,000) * 100\% = 8{,}63\%$$

$$f = (2 * p * r)/(p + r) = 91{,}43\%$$

The results of the fuzzy inference system as a whole are shown in the form of a response surface (fig. 8).

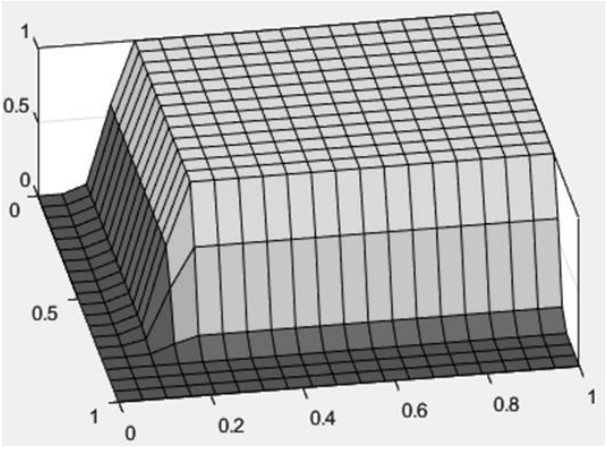

Fig. 8. Work results in the form of a response surface

Based on the determined indicators, it can be concluded that the intruder detection system, developed based on the method of detecting malicious outgoing traffic based on a fuzzy logical conclusion, meets the requirements of public network protection. Reducing the number of first errors can be achieved by expanding the set of network traffic classification rules.

CONCLUSION AND FUTURE DIRECTIONS

The purpose of the study was to improve the security of public networks by detecting malicious and anomalous traffic in them.

In this work, well-known methods of analyzing incoming traffic based on fuzzy logical inference are considered. The goal was to study the parameters based on which traffic analysis is carried out, to find out the problems of these methods.

A model of fuzzy logical inference was proposed to analyze the signatures of outgoing traffic packets. This model provides a comparison of the original packet signatures with the signatures stored in the corresponding dictionaries.

Using a method based on fuzzy logic to analyze the signatures of outgoing traffic packets, the ability to classify outgoing traffic packets to ensure secure connections or block malicious ones is realized.

In the work, the security indicator is determined through the validity metric (F-measure) taking into account the limitations of other validity metrics, as well as taking into account the timeliness and resource requirements. intensity.

Thus, the result of the study should be a combination of different approaches to detect intruders in public networks.

Such an association takes into account the positive approaches existing today, getting rid of their negative aspects as much as possible.

At the same time, the maximization of the F-measure of complex algorithms was achieved under the following metric restrictions: completeness, accuracy, precision; and errors; taking into account requirements for timeliness and resource intensity.

REFERENCES

[1]. Shahid, Usama & Sheikh, Nasir. (2021). Impact of Big Data on Innovation, Competitive Advantage, Productivity, and Decision Making: Literature Review. Open Journal of Business and Management. 09. pp. 586-617. 10.4236/ojbm.2021.92032.

[2]. Vanin, P.; Newe, T.; Dhirani, L.L.; O'Connell, E.; O'Shea, D.; Lee, B.; Rao, M. A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Appl. Sci. 2022, *12*, 11752. https://doi.org/10.3390/app122211752.

[3]. Klots, Y.; Titova, V.; Petliak, N.; Cheshun, V.; Salem, A.-B.M. Research of the Neural Network Module for Detecting Anomalies in Network Traffic. CEUR Workshop Proceedings, 3156, 2022, pp. 378-389. URL: https: // www.scopus.com/authid/detail.uri?authorId=57786856200.

[4]. J. F. Cañola Garcia and G. E. T. Blandon, "A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks," in *IEEE* Access, vol. 10, pp. 83043-83060, 2022, doi: 10.1109/ACCESS.2022.3196642.

[5]. M. Almseidin, J. Al-Sawwa and M. Alkasassbeh, "Anomaly-based Intrusion Detection System Using Fuzzy Logic," *2021* International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 290-295, doi: 10.1109 / ICIT52682.2021.9491742.

[6]. Mansoor Farooq, "Supervised Learning Techniques for Intrusion Detection System based on Multi-layer Classification Approach" International Journal of Advanced Computer Science and Applications (IJACSA), 13(3), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130338.

[7]. Sajad Einy, Cemil Oz, Yahya Dorostkar Navaei, "The Anomaly and Signature-Based IDS for Network Security Using Hybrid Inference Systems", Mathematical Problems in Engineering, vol. 2021, Article ID 6639714, 10 pages, 2021. https:// doi. org /10.1155/2021/6639714.

[8]. Caichang Ding, Yiqin Chen, Zhiyuan Liu, Ahmed Mohammed Alshehri and Tianyin Liu. Fractal characteristics of network traffic and its correlation with network security. Fractals, Vol. 30, No. 2 (2022) 2240067 (11 pages). DOI: 10.1142/S0218348X2240-0679.

[9]. Serhii Toliupa, Ivan Parkhomenko, Ruslana Ziubina, Olga Veselska, Stanislaw Rajba, Kornel Warwas. Detection of abnormal traffic and network intrusions based on multiple fuzzy rules, Procedia Computer Science, Volume 207, 2022, pp. 44-53, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.09.036.

[10]. Amrutha Muralidharan Nair and R Santhosh, "Mitigation of DDoS Attack in Cloud Computing Domain by Integrating the DCLB Algorithm with Fuzzy Logic" International Journal of Advanced Computer Science and Applications (IJACSA), 13(10), 2022. http: // dx.doi.org/10.14569/IJACSA.2022.0131059.

[11]. Ibrahimov, B.G., Alieva, A.A. (2021). Research and Analysis Indicators of the Quality-of-Service Multimedia Traffic Using Fuzzy Logic. In: Aliev, R.A., Kacprzyk, J., Pedrycz, W., Jamshidi, M., Babanli, M., Sadikoglu, F.M. (eds) 14th International Conference on Theory and Application of Fuzzy Systems and Soft Computing – ICAFS-2020. ICAFS 2020. Advances in Intelligent Systems and Computing, vol 1306. Springer, Cham. https://doi.org/10.1007/978-3-030-64058-3_97.

[12]. S. S. Kim and A. L. N. Reddy, "Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data," in *IEEE/ACM* Transactions on Networking, vol. 16, no. 3, pp. 562-575, June 2008, doi: 10.1109/TNET.2007.902685.

МЕТОД АНАЛІЗУ СИГНАТУР ПАКЕТІВ ВИХІДНОГО ТРАФІКУ

Для виявлення вихідного зловмисного трафіку розроблено метод на основі нечіткого логічного висновку для аналізу сигнатур вихідного трафіку. Результати дослідження свідчать про те, що варто продовжувати діяльність у цьому напрямку, щоб розвантажити ресурси мережі під час пікових навантажень. Метод перевіряє підпис пакета вихідного трафіку відповідно до набору правил. Ключовими завданнями методу є: дозвіл з'єднання, якщо під час класифікації підпис пакету визначено як дозволений; блокування з'єднання, якщо під час класифікації визначено, що підпис пакету заборонений; додавання нових підписів до існуючих словників. В ході експерименту метод підтвердив свою ефективність. Наявність методу на основі нечіткої логіки для сигнатурного аналізу вихідних пакетів трафіку має низку переваг, включаючи виявлення раніше невідомих атак, зменшення загальної кількості кібератак, запобігання перевантаженню мережевого обладнання та зниження ймовірності компрометації. поточна мережа.

Ключові слова: нечітка логіка, аналіз сигнатур, вихідний трафік, класифікація сигнатур.

Петляк Наталія Сергіївна, аспірант кафедри безпеки інформаційних технологій, Національний авіаційний університет; асистент кафедри кібербезпеки, Хмельницький національний університет.
Nataliia Petliak, PhD Student of IT-Security Academic Department, National Aviation University; Assistant of Department of Cyber Security, Khmelnytskyi National University.
E-mail: npetlyak@khmnu.edu.ua.
Orcid ID: 0000-0001-5971-4428.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, професор, професор кафедри Інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету.
Yuliia Khokhlachova, candidate of technical sciences, professor, professor of the department of software engineering and cyber security of the State University of Trade and Economics.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

DOI: 10.18372/2410-7840.26.18842
УДК 004.056.5:327.88(470+571):477)

АНАЛІЗ СУЧАСНОГО СТАНУ КІБЕРАТАК В УКРАЇНІ ПІД ЧАС ВІЙНИ

Святослав Храмов, Іван Опірський

Актуальність проблеми кібербезпеки в Україні надзвичайно висока в контексті повномасштабного вторгнення. За останні роки кібератаки стали невід'ємною частиною гібридної війни, яка ведеться проти країни. Дослідження сучасного стану кібергресії в Україні є важливим завданням з погляду національної безпеки. Ця наукова робота має на меті ретельно проаналізувати структуру, тенденції та особливості кібератак, які спрямовані проти України під час військового конфлікту. Дослідження передбачає аналіз різноманітних форм і методів кібергресії, вивчення їхнього впливу на державу та ідентифікацію можливих заходів для захисту критичних інформаційних інфраструктурних об'єктів. Результати дослідження можуть послужити основою для розробки та впровадження ефективних стратегій з кібербезпеки, спрямованих на покращення захисту інформаційної безпеки країни в умовах військового конфлікту. Актуальність цієї роботи полягає в її потенційній здатності допомогти українському уряду та органам безпеки ефективно реагувати на виклики військового конфлікту в кіберпросторі. Для підтримки дослідження було проведено широкий аналіз літератури та статей, які надають інформацію про кібератаки під час війни. Крім того, були використані емпіричні дані про кіберінциденти, зафіксовані в Україні з початку конфлікту, що дозволило детально оцінити масштаби та специфіку загроз. Особливу увагу приділено аналізу типів кібератак, їх тактичних і стратегічних цілей, а також методів, які використовуються для їх реалізації. Дослідження також виявляє основні вразливості, які використовуються зловмисниками, і пропонує можливі шляхи їх усунення. Серед основних типів атак розглядаються DDoS-атаки, фішингові атаки, впровадження шкідливого програмного забезпечення, SQL-ін'єкції та інші. Крім того, розглядається вплив кібератак на різні сектори економіки та соціальної сфери, включаючи державне управління, енергетику, фінанси та інфраструктуру. Результати дослідження мають практичне значення для формування державної політики у сфері кібербезпеки. Вони можуть бути використані для розробки рекомендацій щодо підвищення захищеності інформаційних систем, удосконалення нормативно-правової бази та посилення міжнародного співробітництва в цій сфері. Дослідження також підкреслює необхідність підвищення кібергігієни серед населення та покращення підготовки спеціалістів з кібербезпеки.

***Ключові слова**: кібератаки, війна, типи кібератак, успішність кібератак, ІПСО, DDoS-атаки, прогнозування, методи протидії.*

ВСТУП

Постановка проблеми. У сучасному інформаційному суспільстві, де технологічний прогрес стає неодмінною складовою кожного аспекту життя, кіберпростір стає не лише ареною для технологічного розвитку, але й полем боротьби в контексті військового вторгнення рф на територію України. Одним із ключових аспектів цієї нової реальності є кібератаки під час війни, що визначаються використанням технічних засобів для завдання шкоди інформаційно-комунікаційним системам противника. Динамічний розвиток цього феномену викликає необхідність глибокого аналізу сучасного стану кібератак в умовах війни. Дослідження стану кібератак під час війни є актуальним, адже за показними кількість кібер-порушень безпекового стану в України стрімко зросли з початком повномасштабного вторгнення рф. Кібератаки почали використовуватись як елемент військової стратегії, стали загрозою глобальної безпеки, а необхідність кібератак стає критичною складовою військової діяльності та національної оборони. Метою дослідження є глибокий аналіз та систематизація су-