Signature-based Approach to Detecting Malicious Outgoing Traffic

Nataliia Petliak[a], Yurii Klots[a], Vira Titova[a], Viktor Cheshun[a], Artem Boyarchuk[b]

[a] *Khmelnytskyi National University, 11, Instytuts'ka str., Khmelnytskyi, 29016, Ukraine*
[b] *Tallinn University of Technology, Ehitajate tee 5, Tallinn, 12616, Estonia*

Abstract

The authors of the article made an analysis and found out that most network protection systems are aimed at analyzing incoming traffic. In order to detect the original malicious traffic, a method of signature analysis and a system implementing it have been developed. The results of the study are the basis for continuing work in this area with the aim of automating the process of creating signature dictionaries and identifying signature categories. In order to ensure minimal resource costs for system operation during the development of the method based on the Pareto principle, parameters were chosen for the formation of signatures containing the most necessary information when detecting malicious traffic. The method of signature analysis of outgoing traffic performs a real-time comparison of outgoing traffic signatures with a signature dictionary. The main task of the method is an authorization of connections from the allowed list; blocking of connections from the prohibited list; an authorization of connections and marking the packet as unidentified if the packet signature is not in the allowed or prohibited lists. The approach for detecting anomalous outgoing traffic during the experiment demonstrated its effectiveness against known attacks. But it is not adapted to zero-day attacks.

Keywords [1]

Anomaly detection, typical user model, infringer model, packet signature, method of signature analysis of outgoing traffic

1. Introduction

The increase in the number of Internet users and the digitization of society lead to an increase in the number of cyber incidents and cyber attacks [1], including critical infrastructure [2, 3], educational institutions [4]. Cyber attacks negatively affect the functioning of information systems, and their successful implementation leads to significant material losses.

The analysis, carried out in [5], shows that the use of intrusion detection systems, anti-virus software, anti-spyware and encryption mechanisms is not enough to overcome security risks. The deep learning methods, proposed in [6] for searching for malicious software (malware), allow to increase the reliability and efficiency of the search. In addition, the use of Control-Flow Graph (CFG) and Graph Isomorphism Network, presented in [7], take into account the network activity of the infected device, but at the same time outgoing traffic is not taken into account which generates an infected PC outside the current network.

The purpose of this work is to develop a system for detecting malicious outgoing traffic. The article has the following structure. The second section provides a comparative overview of signature analysis methods of network traffic. The third section analyzes the network and the equipment used for its construction. The fourth section presents a model of a typical user based on obtained data

IntelITSIS'2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine
EMAIL: npetlyak@khmnu.edu.ua (N. Petliak); klots@khmnu.edu.ua (Y. Klots); titovav@khmnu.edu.ua (V. Titova); cheshunvn@khmnu.edu.ua (V. Cheshun); artem.boyarchuk@taltech.ee (A. Boyarchuk)
ORCID: 0000-0001-5971-4428 (N. Petliak); 0000-0002-3914-0989 (Y. Klots); 0000-0001-8668-4834 (V. Titova); 0000-0002-3935-2068 (V. Cheshun); 0000-0001-7349-1371 (A. Boyarchuk)

during traffic analysis in an open network segment. The fifth section describes the model of an intruder that may be present in the network. The parameters required for traffic analysis have been selected in the sixth section and optimized for minimal impact on the network during their analysis. The signature of the packet has been formed in the seventh section on the base of the data from the previous section, the model and method of signature analysis of the outgoing traffic have been described. Data for the experiment conducting and its effectiveness have been displayed in the eighth section.

2. Comparative analysis of malicious network traffic detection methods

Existing intrusion detection systems are aimed at protecting one's own network from outside interference, and developments in this area are looking for more effective incident detection methods. Among the well-known technologies there is the use of a multi-level approach to detect attacks using Smart Grid technology [8]. Intrusion detection systems are widely used on the base of the use of a frame for distributed blind intrusion detection by modeling sensor measurements as a graph signal and the use of statistical characteristics of the graph signal [9]. The systems of machine learning are very popular using various approaches as in [10], which are also aimed at protecting the network from outside attacks.

The proposed in [11] deep learning-based multi-agent system for intrusion detection combines the features of multi-agent system approach with the precision of deep learning algorithms. The system is focused on classifying incoming traffic signatures for the main types of network attacks (DoS, R2L, Probe, U2R), but needs to be tested in real network traffic and refined for use with cloud computing, fog computing, and the Internet of Things.

An intrusion detection system [12] based on deep learning and several analyzers allows detecting abnormal traffic in the network, however, the complexity of the system building, significant hardware costs for solving this problem do not allow implementing such a system for open segments of networks with a small and medium number of clients, due to a considerable value. In [13] it is also shown that intrusion detection systems often give false triggerings, which lead to the need for further analysis of the operation of the intrusion detection system and slow down the overall speed of the cyber protection system. The use of machine learning systems makes it possible to increase the reliability of the IDS system [14], however, the significant complication of these systems leads to a significant increase in cost, and will be impractical for implementation in small and medium-sized networks.

The analysis of the possibility of detecting DoS and DDoS attacks was carried out in [15] on the base of the analysis of the content of packet headers, however, such a system is considered for detecting attacks on the system from the outside. The theory tools of fuzzy sets [16], which are used in determining the level of enterprise security, do not take into account the possibility of attacks from the enterprise network. The use of neural networks [17, 18] only improves and modernizes existing intrusion detection systems. However, these systems are not intended to detect outgoing malicious traffic from the current network, which may use their capabilities to attack third participants.

The attacks of choosing credentials consist in sequentially sending login and password to a remote system. The analysis carried out in [19] shows that such actions can be identified by analyzing the frequency and type of requests sent to the remote computer.

High efficiency in detecting anomalies in computer systems is shown by self-organized distributed systems, in particular, a system based on the method of principal components [20]. However, the use of distributed systems is not possible in the analysis of public networks, as it assumes anonymity and autonomy of its users.

The botnet detection method, presented in [21], proves the possibility of identifying anomalous traffic on the base of the analysis of information placed in the packet headers. The proposed in [22] approach is based on the analysis of behavior in the system, which is actually an analysis of the traffic of an abnormal node. It is determined that such approaches are promising today and proposed to be implemented.

The considered intrusion detection systems have a variety of innovative solutions that determine their effectiveness in performing an analysis of anomalous incoming traffic. But they have in common

the lack of analysis of outgoing traffic. Conducted research shows that the control of outgoing traffic has the potential to detect the malicious activity in the network of a device affected by malicious software, reduce the total number of cyber attacks by blocking abnormal malicious traffic, prevent overloading of network equipment and reduce the probability of compromising the current network and its owner.

3. Analysis of network architecture and its possible functional

Let us present a typical network configuration (Fig. 1). It consists of several VLAN that are configured with different security policies, including closed VLAN for employees and open VLAN for outsiders. Network equipment used in the network can include routers and managed switches. Their difference during scaling the network will be the number of ports and bandwidth, which ensure stable operation for a larger number of users. Settings related to network security will remain unchanged. They allow you to make a set of measures to protect the network from external attacks and may contain intrusion detection systems or their elements. Wi-Fi point parameters do not affect network security issues, but only technical parameters determine the maximum number of connected clients and data transfer speed.

Commonly, open networks allow unauthorized guest access for connections where both users and intruders can be clients. In the absence of functional for detection of attacks which come from the current network from the third participants, the network may experience a decrease in useful traffic, network compromising and increased delays during data transmission.

User behavior is considered normal by default. Only after the detection of malicious actions of the user, he will move from the group of ordinary users to the group of intruders. It should be noted that attacks may not always be implemented on purpose. There are cases when the user's device is involved in an attack without the user's knowledge. For example, when a device is infected with a virus, has malware installed on it, or is a part of a botnet.

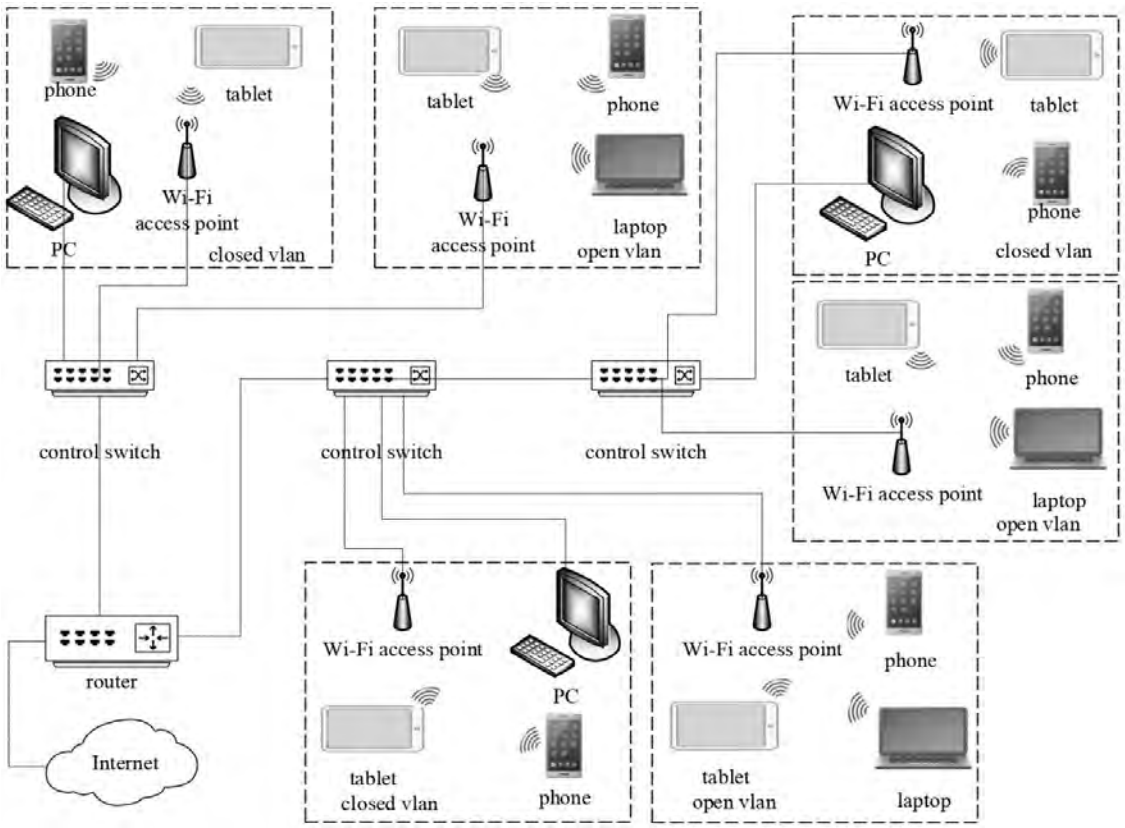

Figure 1: A typical configuration of a corporate network

For the purpose of research, before creating a test network segment, network traffic was observed

and analyzed in an existing open network segment. All users were informed that their traffic would be studied for scientific purposes by receiving a notification on their device and they agreed. The number of connected clients, packet signatures, data transfer rates of clients and the outgoing channel from the subnet were being investigated during one week. It should be noted that a system for detecting intrusions coming from outside the network was connected to the network. The scheme of the network without a system for detecting malicious outgoing traffic is shown in Figure 2. As can be seen from the results of the network analysis (Figure 3), the schedule changes depending on the time of day and day of the week, since the traffic analysis was carried out in university and there are time intervals when the number of users is equal to 0 or significantly lower than the average value. This is related to the specifics of the work.

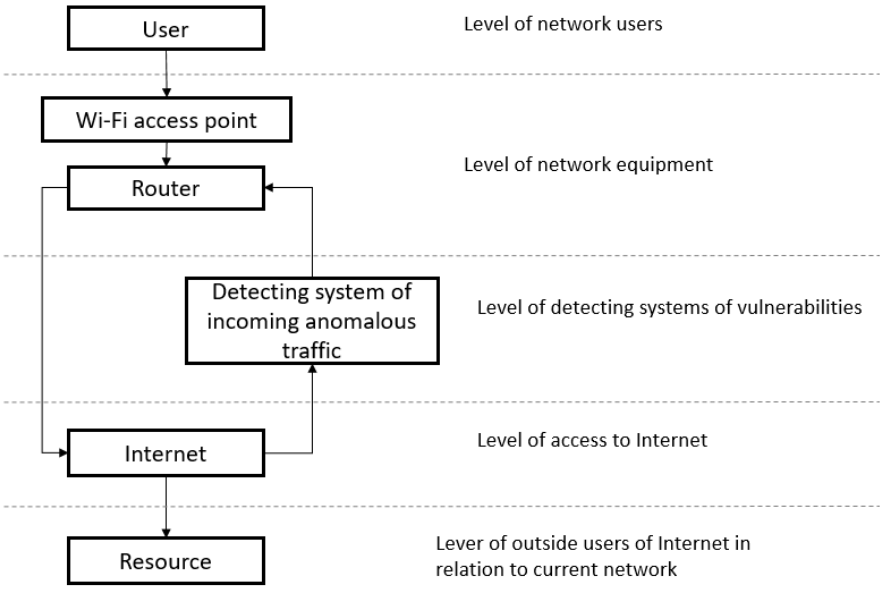

Figure 2: A network diagram without a detecting system of malicious outgoing traffic

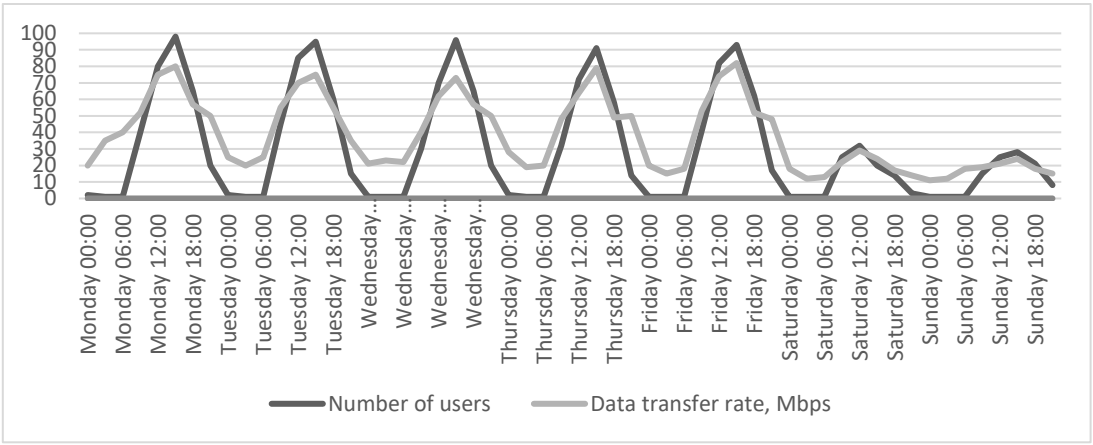

Figure 3: Network analysis regarding the number of users and data transfer rates

4. Behavior model of a typical user

After analyzing user behavior in open segments, the most used applications for typical users were determined:

1. Telegram.
2. Viber.
3. Zoom.
4. Work with search engines.

5. Facebook and Messenger.
6. Postal service.
7. Online banking.

Using of the Telegram application. The use of the IP addresses of two subnets (91.108.4.0/22 and 149.154.167.0/20), the use of ports (80, 88, 8443) is noted in the technical documentation [23]. Table 1 presents a fragment of the network analysis when working with the browser version of the Telegram application and Figure 4 – for the Telegram mobile application. During network monitoring, it was found that while working with the application or the browser version, IP addresses of the source and recipient remain the same, although there may be the least of involved ports. The recipient port will be 443 and the TCP protocol is used. Analyzing the received data, we can conclude that the combination of the IP address of one of the subnets and one of the specified ports is a characteristic feature of working with Telegram and can be considered a good traffic.

Table 1
A fragment of network analysis while working with the browser version of the Telegram application

IP source	Port source	IP destination	Port destination
172.20.110.72	61184	149.154.167.41	443
172.20.110.72	61065	149.154.167.41	443
172.20.110.72	61064	149.154.167.99	443
192.168.16.107	53562	149.154.167.41	443
192.168.16.107	54096	149.154.167.41	443
192.168.16.107	54149	149.154.167.99	443

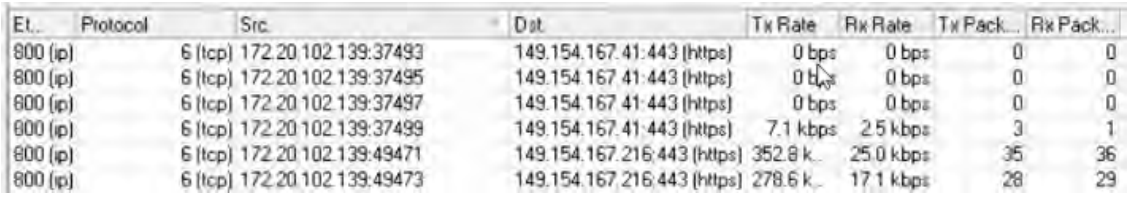

Figure 4: A fragment of the network analysis while working with the version for the Telegram mobile application

Using of the Viber application. Analyzing the data obtained as a result of network monitoring (Table 2), we can conclude that a one-time connection is established between the device and the application server for data exchange. The same combination of IP-address and a port of recipient is used as long as the user is on the current network.

Table 2
A fragment of network analysis while working with the Viber application

IP source	Port source	IP destination	Port destination
172.20.110.72	61099	52.0.252.41	443
52.0.252.41	443	172.20.110.72	61099
192.168.16.107	53597	44.192.202.0	443
44.192.202.0	443	192.168.16.107	53597

Using of the Zoom application. The technical documentation on the developer's website [24] states that IP addresses and ports are clearly defined depending on how resources are used (mobile application, browser, etc.). To configure firewalls, TCP ports 80, 443, 8801, 8802 and UDP ports 3478, 3479, 8801-8810 are used. TCP ports 5091, 390 and UDP from the range 20000-64000 are used in the work with the Zoom mobile application. According to the firewall rules for Zoom Contact Center, UDP ports from the range 20000-64000 and TCP 443, 5091 are used. The firewall uses TCP ports 80, 443 and no longer defined IP addresses but the domain *.zoom.cloud in the application

through a browser. Firewall rules for Zoom apps use TCP ports 443 and the *.zoomapp.cloud domain.

After studying the behavior of network traffic while working with the Zoom application (Table 3), we can monitor the connection to the subnet in the range of IP addresses and the use of the port, which confirms the data from the documentation.

Work with search engines. Ports 80, 443 and the IP address corresponding to one or another site (Table 4 and Figure 5) are mostly used while working with search engines.

Table 3

Fragment of network analysis while working with Zoom

IP source	Port source	IP destination	Port destination
172.20.110.72	51800	170.114.52.4	443
172.20.110.72	51800	170.114.52.4	443
172.20.110.72	61128	170.114.15.95	443
192.168.16.107	63924	170.114.2.8	443
192.168.16.107	63954	170.114.14.58	443
192.168.16.107	63914	170.114.52.3	443
192.168.16.107	63972	170.114.15.226	443
192.168.16.107	63960	170.114.35.162	443

Table 4

A fragment of network analysis while working with search engines using a laptop

IP source	Port source	IP destination	Port destination
172.20.110.72	61166	35.245.210.119	443
172.20.110.72	61473	216.58.209.16	443
172.20.110.72	61505	18.66.121.64	443
172.20.110.72	61151	173.194.73.188	80
172.20.110.72	61504	142.250.203.197	443
172.20.110.72	61504	142.250.203.197	443

Et...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	172.20.102.139:40258	159.203.145.121:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:40260	159.203.145.121:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:40268	159.203.145.121:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:40276	157.240.224.7:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:40357	157.240.224.7:443 (https)			240.7 k...	9.2 kbps	25	14
800 (ip)	17 (udp)	172.20.102.139:40428	142.250.186.193:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:40879	104.26.7.133:443 (https)			4.1 Mbps	174.0 k...	460	81
800 (ip)	17 (udp)	172.20.102.139:40969	34.117.98.198:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:41043	104.21.52.152:443 (https)			6.7 Mbps	100.3 k...	689	119
800 (ip)	6 (tcp)	172.20.102.139:41465	157.240.224.12:443 (https)			776 bps	0 bps	1	0
800 (ip)	6 (tcp)	172.20.102.139:41467	157.240.224.12:443 (https)			776 bps	0 bps	1	0
800 (ip)	6 (tcp)	172.20.102.139:41671	157.240.224.12:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:41730	216.58.215.100:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:41878	35.186.231.97:443 (https)			44.7 kbps	9.4 kbps	8	9
800 (ip)	17 (udp)	172.20.102.139:41889	172.20.0.2:53 (dns)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:42150	172.20.0.2:53 (dns)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:42335	18.66.233.2:443 (https)			91.3 kbps	16.7 kbps	17	14
800 (ip)	6 (tcp)	172.20.102.139:42436	78.152.183.46:443 (https)			15.8 Mbps	371.9 k...	1317	688
800 (ip)	17 (udp)	172.20.102.139:42450	142.250.186.200:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:42868	18.66.233.57:443 (https)			47.2 kbps	19.2 kbps	8	8
800 (ip)	6 (tcp)	172.20.102.139:42953	172.67.75.202:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:43103	142.250.203.206:443 (https)			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:43196	142.250.203.206:443 (https)			0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:43285	172.20.0.2:53 (dns)			0 bps	0 bps	0	0

Figure 5: A fragment of network analysis in the work with search engines using a mobile phone

Using of Facebook and Messenger applications. TCP and UDP protocols are used in the Facebook and Messenger applications (Figure 6), depending on the performed actions, a one-time connection is established to a certain IP address, and port 443 is used.

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	172.20.102.139:37605	157.240.224.7:443 (https)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:37627	157.240.224.7:443 (https)	47.8 kbps	12.1 kbps	14	11
800 (ip)	6 (tcp)	172.20.102.139:37629	157.240.224.7:443 (https)	31.6 kbps	6.6 kbps	7	8
800 (ip)	6 (tcp)	172.20.102.139:37854	157.240.224.16:443 (https)	0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:40404	157.240.224.63:443 (https)	631.2 k...	8.5 kbps	64	8
800 (ip)	17 (udp)	172.20.102.139:40869	157.240.224.63:443 (https)	126.9 k...	74.6 kbps	28	19
800 (ip)	6 (tcp)	172.20.102.139:40902	157.240.224.63:443 (https)	0 bps	0 bps	0	0
800 (ip)	17 (udp)	172.20.102.139:47288	157.240.224.63:443 (https)	0 bps	0 bps	0	0

Figure 6: Fragment of network analysis while working with Facebook and Messenger applications

Using of the application of a popular mail service. When using the application (Figure 7) or the site, a one-time connection is established with the IP address and only its use in combination with port 443, the ports of the mobile device may change. TCP protocol is used.

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	172.20.102.139:37449	89.184.85.91:443 (https)	5.4 kbps	8.3 kbps	1	2
800 (ip)	6 (tcp)	172.20.102.139:37457	89.184.85.91:443 (https)	5.9 kbps	7.6 kbps	2	2
800 (ip)	6 (tcp)	172.20.102.139:37459	89.184.85.91:443 (https)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	172.20.102.139:37465	89.184.85.91:443 (https)	4.4 Mbps	10.5 kbps	369	20

Figure 7: A fragment of the network analysis while working with the mail service application

Using of one application from the online banking. While working with the bank application (Figure 8), the TCP protocol and recipient port 443 are used similarly to the previous points. But depending on the operations performed by the user, the IP addresses change. For example, the transaction archive is stored at one address, and other addresses are used while transferring funds or viewing the account status.

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	172.20.102.139:40827	3.72.18[illegible].443 (https)	6.3 Mbps	134.2 k...	527	245
800 (ip)	6 (tcp)	172.20.102.139:40831	3.72.1[illegible].443 (https)	3.3 Mbps	71.3 kbps	280	126
800 (ip)	6 (tcp)	172.20.102.139:46869	3.65.1[illegible].443 (https)	592 bps	592 bps	1	1
800 (ip)	6 (tcp)	172.20.102.139:46873	3.65.1[illegible].443 (https)	1120 bps	2.1 kbps	2	4
800 (ip)	6 (tcp)	172.20.102.139:48005	52.31.1[illegible].443 (https)	4.7 kbps	2.4 kbps	2	3
800 (ip)	6 (tcp)	172.20.102.139:48213	52.223.1[illegible].443 (https)	111.8 k...	11.4 kbps	19	12
800 (ip)	6 (tcp)	172.20.102.139:48215	52.223.1[illegible].443 (https)	42.2 kbps	6.7 kbps	8	9
800 (ip)	6 (tcp)	172.20.102.139:48217	52.223.1[illegible].443 (https)	42.2 kbps	6.7 kbps	8	9
800 (ip)	6 (tcp)	172.20.102.139:48219	52.223.1[illegible].443 (https)	42.2 kbps	6.7 kbps	8	9

Figure 8: A fragment of the network analysis while working with the bank application

So, on the base of the available observations and researches, it can be concluded that the connection can be considered safe with a combination of protocols, certain (typical) IP addresses and the corresponding recipient ports, and this data can be taken as good traffic and always allowed on the network.

5. Behavior intruder`s model

After the model of a typical user has been defined, it is necessary to determine the models of intruders for different types of attacks and to investigate the typical behaviour of malicious traffic and we should develop a typical model of the intruder.

Behavior of the intruder when attacking the password. Access attacks, particularly attacks on passwords, are increasingly being carried out because the number of accounts and the value of the information they contain have increased significantly after the transition to digitalization. While implementing such an attack, in most cases, there is an attack on standard services and standard ports (Table 5). Brute force, dictionary matching, and pattern checking are the methods of common password cracking.

Table 5
Use of protocols and ports when attacking passwords

Using a pair of protocols	Attacks on ports
SSH i TCP	22, 80
PPTP i TCP	1723
L2TP i UDP	500, 1701, 4500
RDP i TCP	3389
VNC i TCP	5900

An example of network traffic from the intruder's side when trying to select a login and password for a site on the CMS Wordpress, collected using the Wireshark program, is shown in Figure 9.

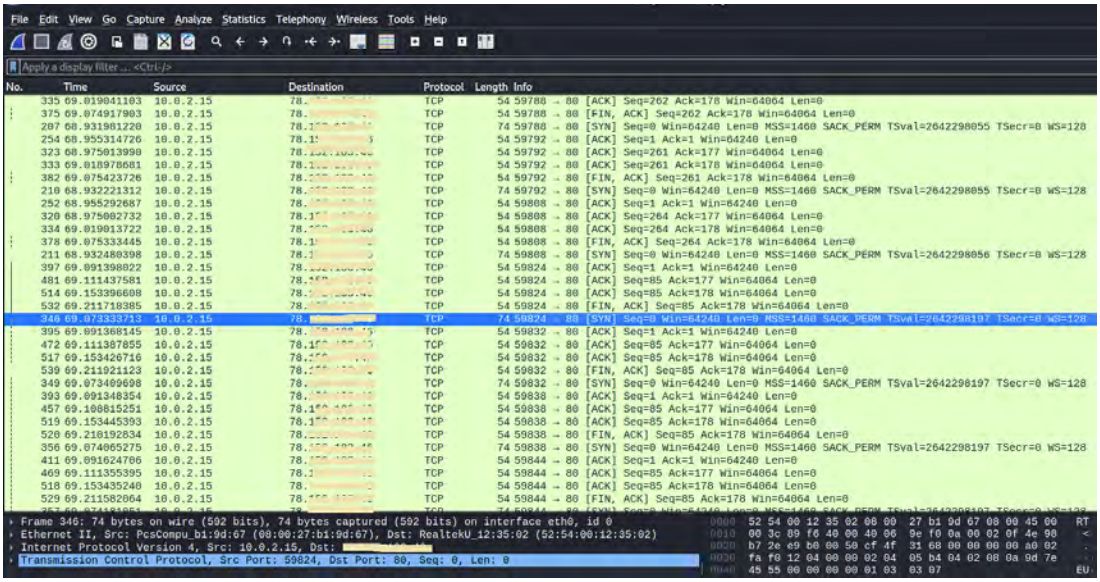

Figure 9: Network traffic from the intruder's side when trying to select a login and password

During such an attack, the stages of execution of the attack by the intruder will be formed in the following way:

1. Preparation for the attack. At this stage, the intruder chooses the object of the attack, according to his own motives, and collects the necessary information, including the help of social engineering.
2. Development of an attack plan. The intruder identifies the network to which he will join to carry out the attack and the way to carry out the attack, prepares dictionaries or configures the software.
3. Implementation. The intruder joins an open network segment and launches a direct attack. During this attack it is possible to detect the fact of violation based on traffic analysis. To do this, while scanning the outgoing network traffic, you should analyze the incoming and outgoing ports and IP addresses, the frequency of calls, and the protocol. The time to choose a password directly depends on the entropy of the password and on the device from which the attack is launched, and the speed of the network from which the attack is started.
4. After the successful fulfillment of the attack, the user can use the received data depending on the previously defined motives.
5. The intruder may try to hide information about his actions from the object of the attack.
6. The intruder leaves the already compromised network.

It should be noted that points 1, 2, 4, 5, 6 are not identified by traffic analysis, because they are similar to the actions of a normal user. Based on the previously presented material, we will create a model of the intruder for this type of attack, which is shown in Figure 10.

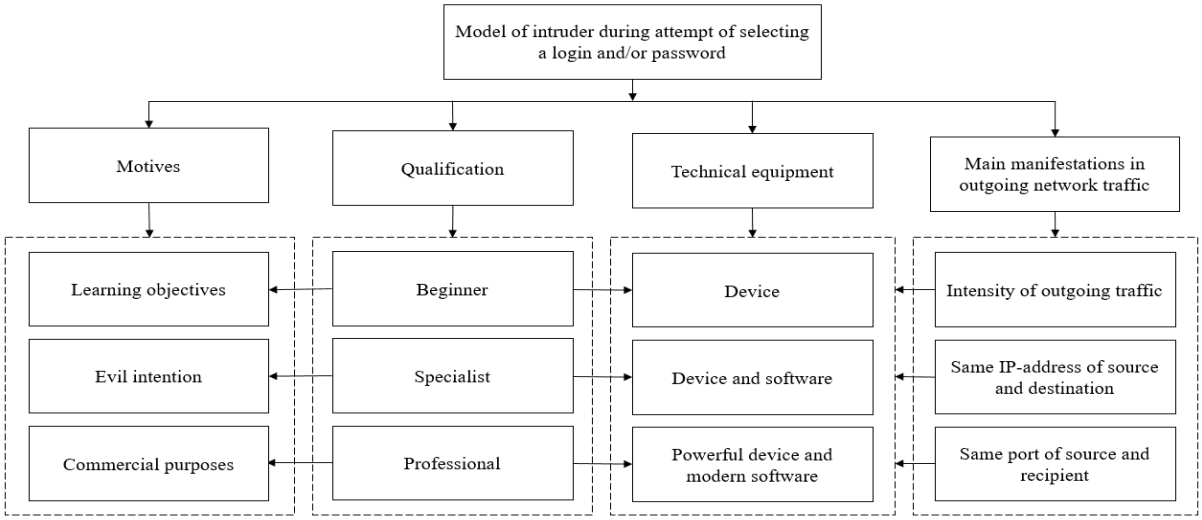

Figure 10: Model of the intruder during a password attack

Model of the intruder during the attack on a denial of service. Despite the simplicity of implementation and the existence of basic rules for protection against the attack, the popularity of this attack does not decrease. After all, actions can be taken not only to root servers or IPs, but also to certain parts that perform vital tasks or to places where security "holes" were previously found.

In the process of analyzing the ICMP flood in the network traffic, we can observe the same type of ICMP ECHO requests, which will have the same recipient address. It is worth noting that the requests will come at the same interval. But the interval of sending requests is configured by the intruder before starting the attack. We should also pay attention to the size of the package. Exceeding the packet size can crash the server if it is not configured for packet fragmentation.

A SYN flood initiates a large number of simultaneous TCP connections by sending a SYN packet with a nonexistent return address. For a more effective attack, the intruder can first conduct a reconnaissance attack in order to identify the most vulnerable network nodes. After the attack is successfully implemented, the target of the attack stops functioning due to the large number of unsent responses and drops all new connections.

UDP flood during analyzing network traffic is tracked due to a large number of UDP packets to different ports with the same IP address.

HTTP messages GET with high intensity on port 80 characterize an HTTP flood attack. Its main purpose is to load the key elements of the system to a state where they will not be able to handle any other requests.

During a Ping of Death attack an intruder tries to stop or crash a server by sending a normal ping request that is either fragmented or oversized. When a ping greater than the maximum size is sent, the target server will fragment the file. Later, when the server formulates a response, reassembling of this larger file can cause a buffer overflow and crash. When analyzing traffic, this type of attack can be traced by the size of the packet and its components.

DoS attacks from the intruder's side are somewhat similar to port scanning if we analyze network traffic, including the time and protocols used. However, we can set the intensity of the attack, specify the number of requests and refuse to receive a response. These parameters are the main ones to detect a network traffic during analyzing.

So, the model of the intruder during the attack of denial-of-service will look according to Figure 11.

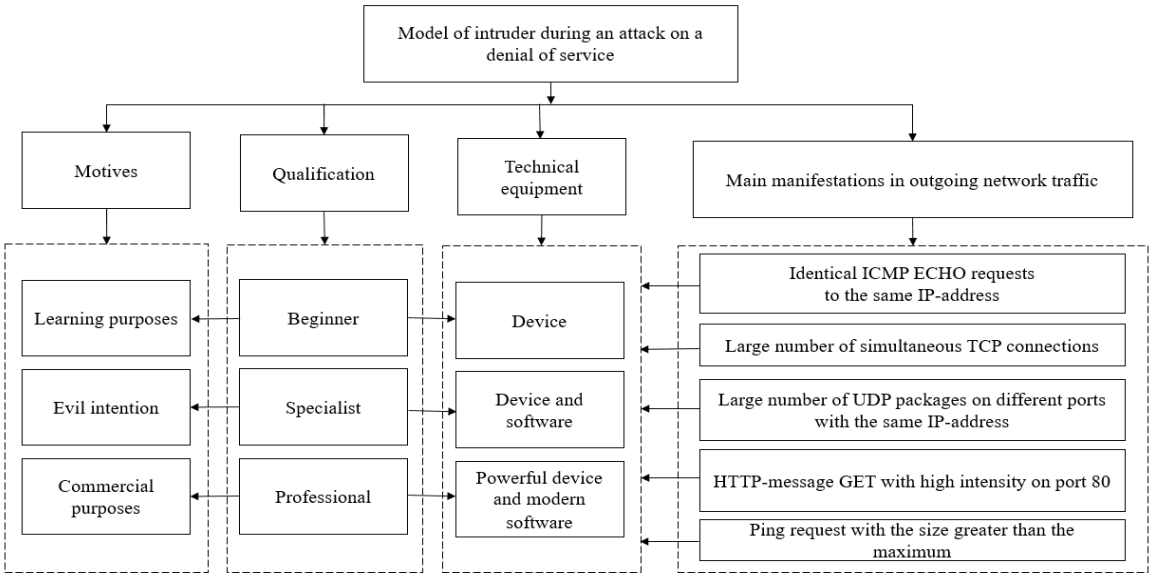

Figure 11: Model of the intruder during the attack on a denial of service

A model of an intruder during reconnaissance attacks. During reconnaissance attacks, the intruder attempts to discover active network nodes, so he sends ping requests to the entire range of IP addresses of the network he wants. Usually, tools for deploying ping requests are used, which sequentially go through all the IP addresses of the network one after the other. While scanning IP addresses, a certain number of requests are sent to each address. The absence of one response does not yet indicate its disabled state or absence from the network, because it could be busy with another request at that time. The time interval to make requests to the same address and the number of requests for each scan may differ, because the intruder can easily change them based on needs and capabilities. For example, a large number of simultaneous requests going through one network device can disable the network equipment, but the intruder will not get the desired result. Therefore, scanning by IP addresses is "stretched" in time to obtain the desired result. During the scanning, ARP protocol is used for the request and ICMP is used for the reply if the address is available (working, enabled).

When the IP address is identified as working, the port scanning process can begin. During it, one IP address is used, only the port numbers change (usually during scanning the range of ports 0-1023 is used). The number of streams of address and port scans can be configured by the intruder depending on the bandwidth of the network. Network traffic from the intruder's side during port scanning is shown in Fig 12.

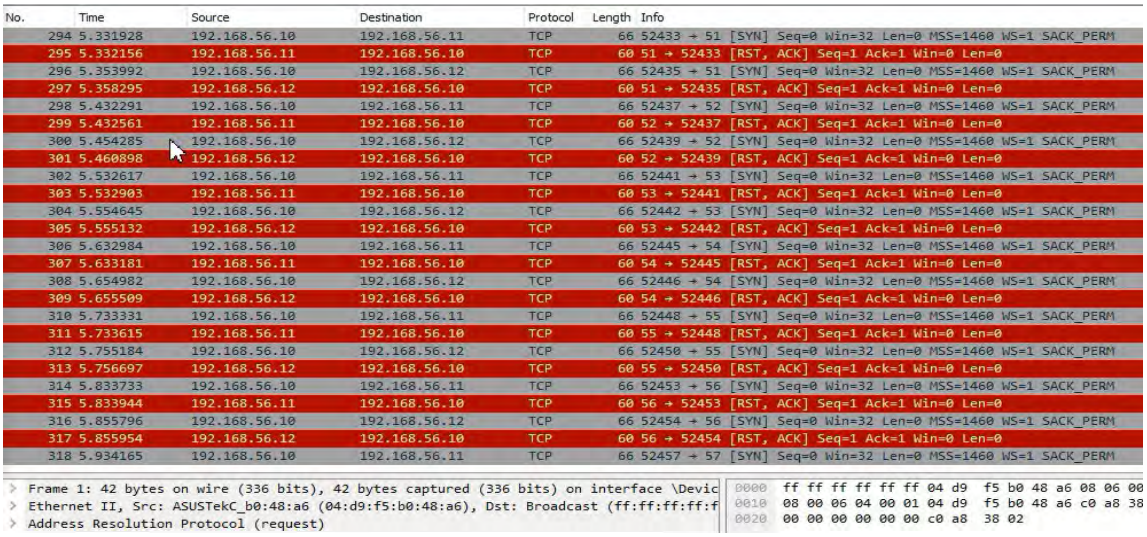

Figure 12: Network traffic from the intruder's side while polling ports

During collecting information about the host-victim using active scanning, the intruder sends requests to the host address using all possible protocols and receives responses. The main goal is to

search for open databases or ports, analyze the software in use and the network structure in order to identify vulnerabilities for further malicious actions.

The stages of the attack will be similar to the model of the intruder when attacking the password, except for the third point. For the current attack it will be as follows:

- The offender joins an open network segment and runs a program to scan IP addresses.
- If the IP address gives a response, then port scanning is started at this address.

During traffic analysis, these activities will show up in consecutive recipient IP addresses and a large number of requests to a single IP address using a specific port range in sequence. Therefore, the model of the violator can be depicted as in Figure 13.

Model of the intruder during setting up remote work. Many attacks are carried out through the use of malicious software or by changing the account privileges of the system that the intruders are trying to affect. However, it is quite difficult to trace such attacks by analyzing the outgoing network traffic because the search for known signatures of the malware in the analysis of the data of the packet content is a long-term process compared to simply transmitting the packet. Therefore, it will be an additional load on the network equipment, slowing down the operation of the entire network. But a characteristic sign of the beginning or intention of malicious actions is the setting of remote access to a computer or any other device located outside the network which is analyzed. That is why we should monitor the protocols that were used during the connection.

On the base of the research of this problem (Figure 14) we can say that SSL, TPKT, TCP, RDP-UDP protocols mainly function during working with a remote device.

The stages of implementing attacks using a remote desktop will be similar to the stages of implementing an attack on a password. On the basis of the obtained data, we build the model of the intruder shown in Figure 15.

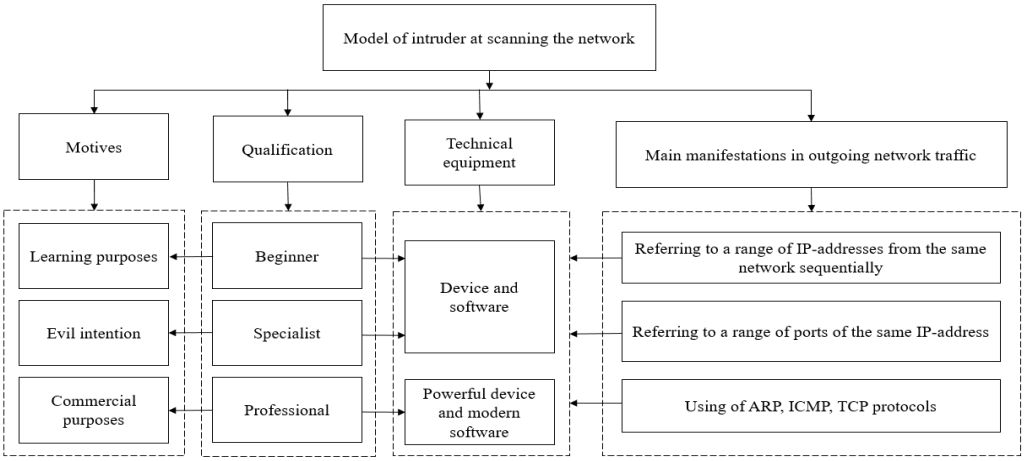

Figure 13: Model of the intruder at scanning the network

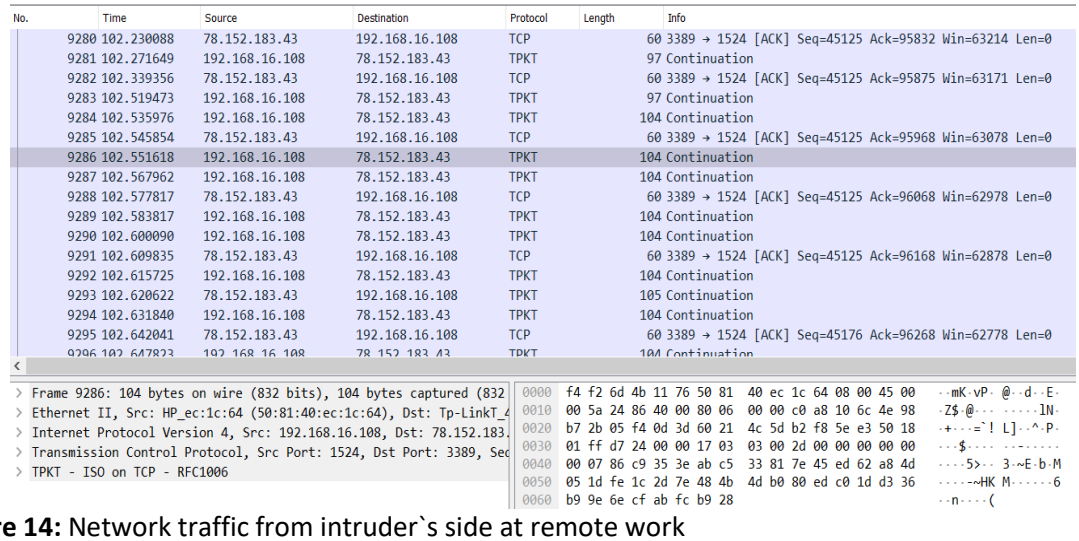

Figure 14: Network traffic from intruder`s side at remote work

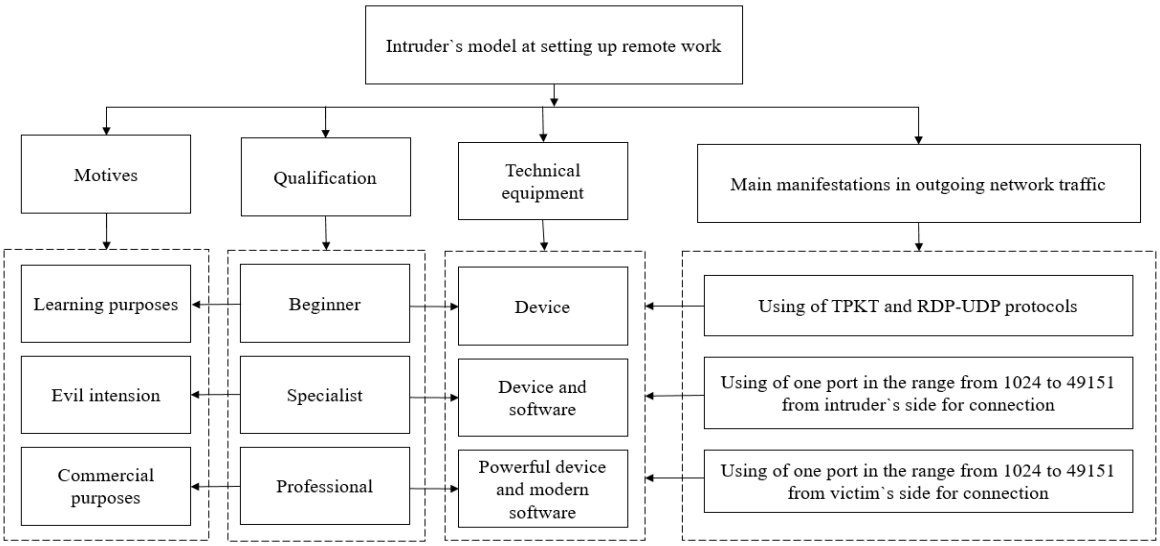

Figure 15: Intruder`s model at setting up remote work

Model of the intruder during sending spam via e-mail. E-mail for sending spam is used not only for advertising purposes by various organizations, where various linguistic means are actively used and the owner of the mailbox could register on a certain site or make an order. Also, while sending emails, links for phishing attacks may be sent, or they may contain attachments that are malware. Mostly, the topics of the letters in such cases are popular or socially important. According to CERT-UA, the following topics prevailed in emails with malicious content in 2022: monetary payments, assistance from the Red Cross and on behalf of the State Service of Special Communications and Information Protection of Ukraine, Security Service of Ukraine or other authorities.

Mail spam can be traced through a large number of requests to one or more mail servers during analyzing network traffic, since the letters do not go directly to the recipient. Also, the use of the SMTP protocol from port 25 to port 25, as this is the service port responsible for e-mail transmission between mail servers.

During such an attack, the stages of attack implementation by the intruder will be formed in the following way:

1. Preparation for the attack. At this stage, the intruder will collect the addresses for the mailing. Collecting addresses can be done by various methods: from buying customer bases to parsing sites with job search.
2. Development of an attack plan. The intruder identifies the network to which he will join to carry out the attack and he identifies the method of sending messages. The maximum possible limit of sent letters per day depends on the postal service. If it is a free mailing from the site, then the limit will reach 500 letters per day. If it is a regular mailbox, then 5,000 letters per day. These values are specified by default and can be adjusted. For paid profiles, the number of letters per day depends on the tariff. But at the same time, we should be taken into account the disclosure of information about the attacker, according to which he will carry out registration and payment. Also, before starting the attack, the text must be prepared. In order to change automatically the subjects of the letters and to make it more difficult to identify the letter as spam, intruders can use the malware.
3. Implementation. An intruder joins an open network segment and launches a direct attack. During this attack it is possible to detect the fact of violation based on traffic analysis. To do this, when scanning the outgoing network traffic, we should analyze the incoming and outgoing ports and IPs, frequency of calls, ports. The speed of mailing directly depends on the number of letters that will be sent and network capabilities.
4. After the successful completion of the attack, the intruder tries to hide the signs of his participation in sending letters and expects actions from the recipients. It can be a link or a launch of the malware.

On the basis of the previously presented material, we will create a model of the intruder (Figure 16).

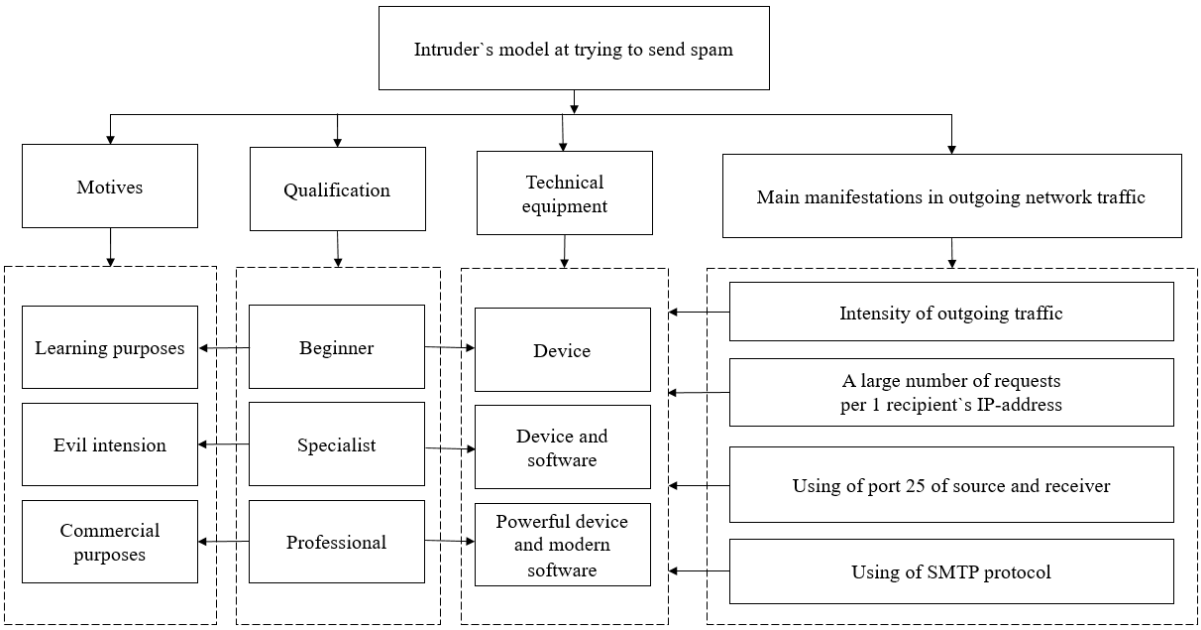

Figure 16: Intruder`s model at trying to send spam

Let's create a generalized model of the intruder (Figure 17), which describes the main motives, the level of qualification of the intruder, possible options for technical equipment, and the main manifestations of attacks in network traffic.

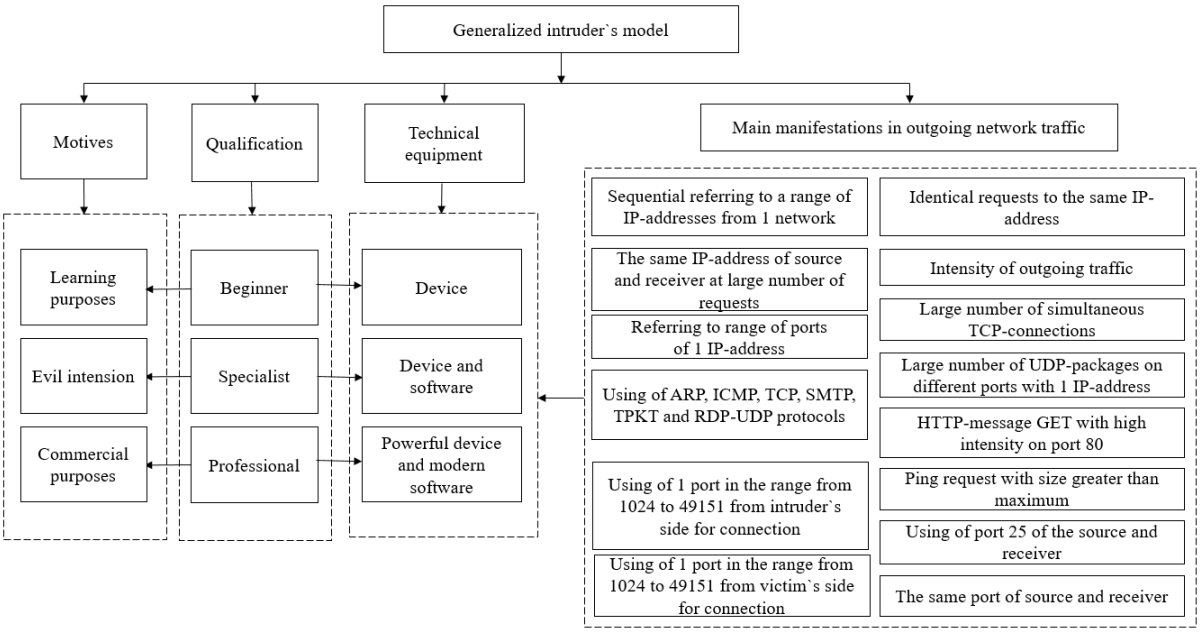

Figure 17: Generalized model of the intruder

6. Selection of features for traffic analysis and their optimization

Since most of the content of the packet is occupied by data, only headers were used for traffic analysis. Let's present a graph of the dependence of header elements on types of attacks (Figure 18).

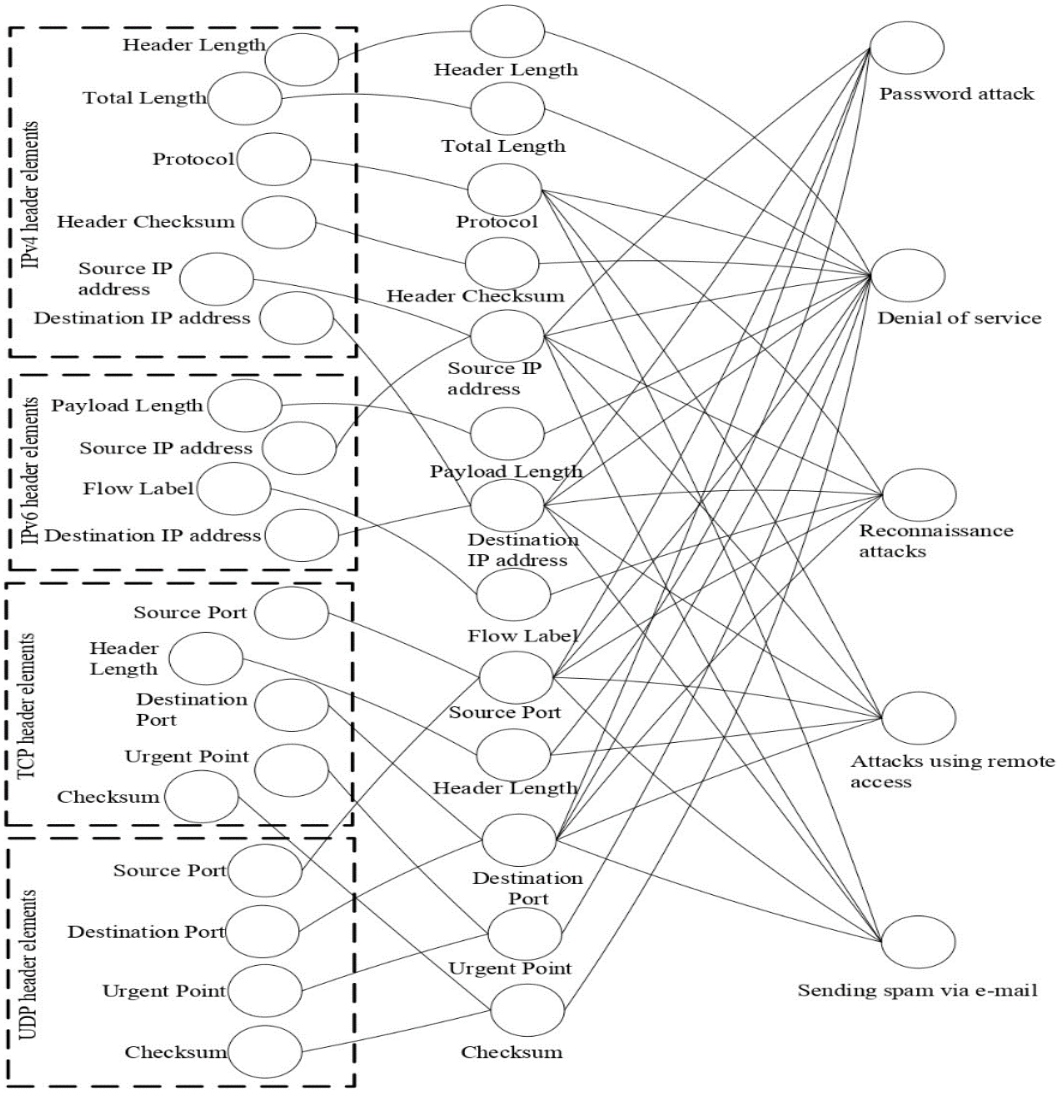

Figure 18: The graph of the dependence of header elements on attack types

The graph shows that some of the headers are not used during traffic analysis. This is due to the fact that they contain exclusively service information or their analysis will cause an additional load on the system.

A large number of parameters will require more computing power to implement the analysis and will increase data transfer delays. Therefore, it is advisable to choose parameters with the greatest efficiency in order to maintain stable operation of the network. Let's use the Pareto principle (Figure 19), according to which 20% of parameters provide 80% of efficiency [25]. Since 5 types of attacks were analyzed during the formation of the intruder model, y=5 is the maximum value provided that the feature is used to detect malicious traffic in each of the types of attacks. Accordingly, y=0 if the feature was not used for detection at all. It should be noted that this analysis will show the data transfer rate indicator, which is not in the packet header, but which affects the detection of traffic anomalies. The diagram shows that it is optimal to use the following parameters: source ports and recipient ports, IP addresses of source and recipient, protocol, data transfer rate. Therefore, it is necessary to optimize the graph shown in Figure 8. We present it in Figure 20.

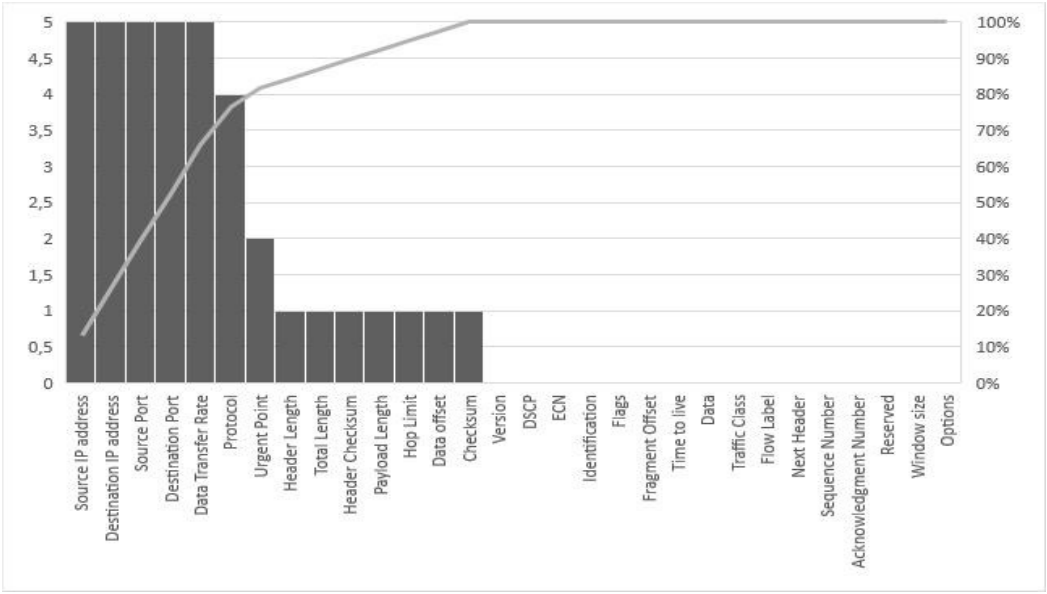

Figure 19: Diagram of parameter selection for traffic analysis using the Pareto principle

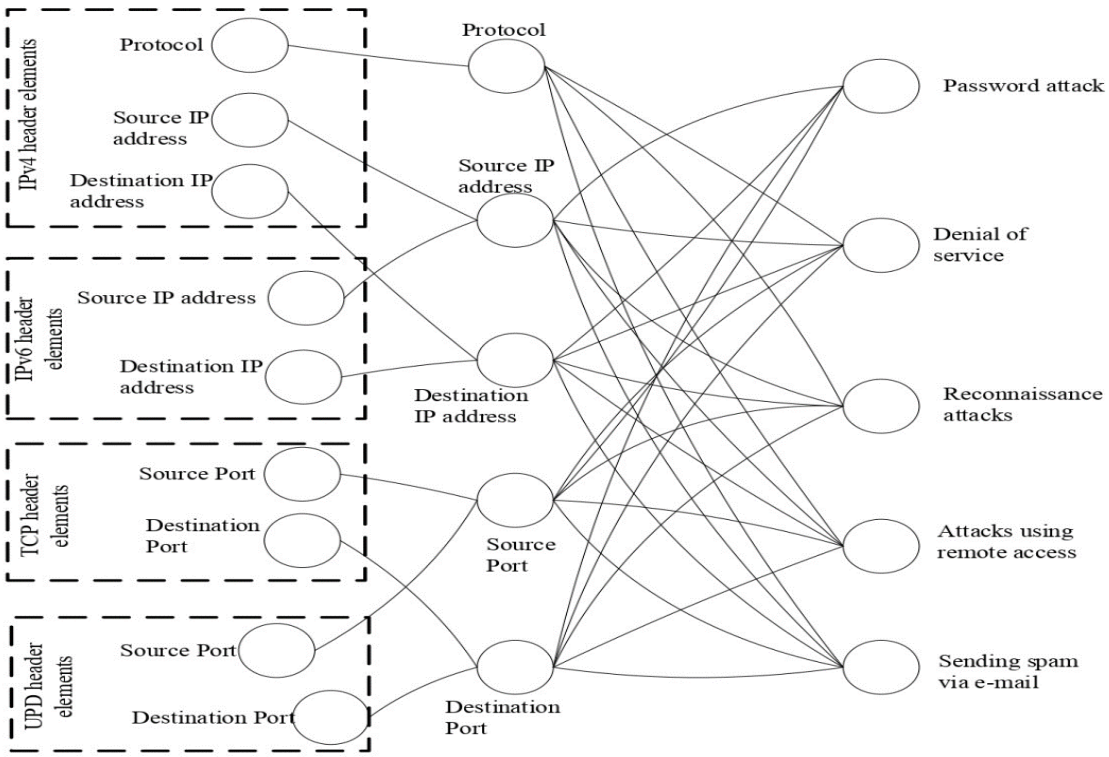

Figure 20: Optimized graph of dependence of header elements on types of attacks

7. Signature of the Package

Let's create a package signature, which is needed for further package analysis. The package signature will be presented in the following way:

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

where *IPs* – IP-address of the source specified in the package header IPv4/IPv6;
IPd – IP-address of allocation specified in the package header IPv4/IPv6;
Ps – port of the source noted in TCP/UDP-header;
Pd – port of allocation noted in TCP/UDP-header;
Pr – protocol noted in the header of a package IPv4;

Sd – data transfer rate.

The package signature will allow you to uniquely identify the traffic source, the application that initiates it, and determine the data transfer rate.

Let`s present the set of input signatures as a plural:

$$D = \{s_i\}_{i=0}^{N_d}, \quad (2)$$

where s_i – set element, input generated signature;

i – initial value;

N_d – the number of elements of the set.

Each generated signature will belong to a set *D*:

$$\forall s_i \in D \quad (3)$$

In order to quickly and effectively analyze the traffic, we will generate sets of signatures of permitted (*G*) and prohibited (*B*) traffic, undefined (*U*).

Let`s present the set of allowed traffic in following way:

$$G = \{s_i\}_{i=0}^{N_g}, \quad (4)$$

where *G* – set of allowed traffic;

s_i – element of the set;

i – initial value;

N_g – number of elements of the set.

Packages whose signature belongs to the set *G*, should be passed without further inspection.

We present the set of malicious traffic as follows:

$$B = \{s_i\}_{i=0}^{N_b}, \quad (5)$$

B – set of malicious traffic;

s_i – element of the set;

i – initial value;

N_b – number of elements of the set.

Packets whose signature belongs to set *B* should be dropped without further inspection.

We present the set of undefined traffic as:

$$U = \{s_i\}_{i=0}^{N_u}, \quad (6)$$

B – set of undefined traffic;

s_i – element of the set;

i – initial value;

N_u – number of elements of the set.

Packets whose signature belongs to the set *U* require further verification.

A set of incoming signatures combines the sets of good, bad, and unknown traffic:

$$D = G \cup B \cup U \quad (7)$$

It is important to note that elements of the set of signatures *G* are not included in the set of signatures *B* and the set of signatures *U*:

$$G \cap B = \emptyset \quad (8)$$

$$G \cap U = \emptyset \quad (9)$$

The elements of the signature set *B* are not included in the signature set *G* and the signature set *U*:

$$B \cap G = \emptyset \quad (10)$$

$$B \cap U = \emptyset \quad (11)$$

The elements of the signature set *U* are not included in the signature set *G* and the signature set *B*:

$$U \cap G = \emptyset \quad (12)$$

$$U \cap B = \emptyset \quad (13)$$

The method of signature analysis of outgoing traffic performs a real-time comparison of outgoing traffic signatures (s_i) against a signature dictionary (*D*). The main task of the method is:

- permission of known good connections if the inspected signature of the packet s_i matches the set *G*:

$$s_i \in G \quad (14)$$

- blocking of known bad connections if the signature of the inspected package s_i matches the set *B*:

$$s_i \in B \quad (15)$$

- marking a package as not identified if the signature of the checked package s_i does not match the

set *G* and the set *B*. Also record of this signature to the set *U*:

$$s_i \notin G \wedge s_i \notin B, mo\ s_i \in U \quad (16)$$

Permission or prohibition of a connection when comparing with existing signatures will not be time-consuming. The method is implemented using a hardware and software component.

The sequence of operation of the method of signature analysis of outgoing traffic (Figure 21).

Step 1. For each package from the traffic, we form a package signature (s_i), where $s_i \in D$.

Step 2. If the signature of the package s_i belongs to the set *G*, then the package is allowed to be transmitted, otherwise the transition to step 3 is made.

Step 3. If the signature of the package s_i belongs to the set *B*, then the package is blocked; otherwise, the transition to step 4 is made.

Step 4. We include the package signature in the set of undefined signatures *U* and allow transmission.

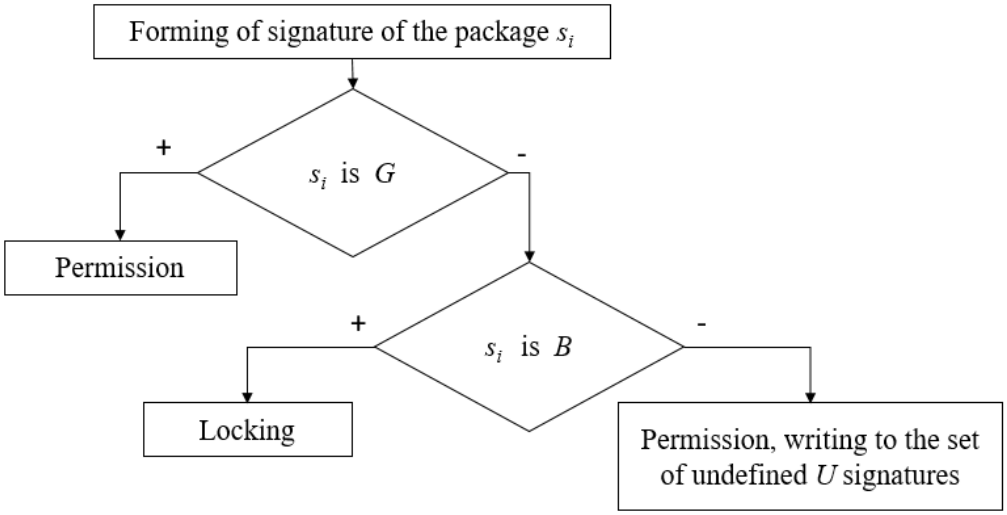

Figure 21: Graphic representation of the operation of the method based on signatures

8. Conducting the experiment and efficiency

An environment for conducting an experiment was implemented as a next step in order to confirm the effectiveness of the described method. The network scheme remained the same (Figure 2), but the number of users changed (there will be a fixed number of 30 people). Connected devices perform typical user actions and are connected during the entire duration of the experiment. The power of the input channel will be 100 Mbit/s, the data transfer speed will reach from 50 to 70 Mbit/s, ping 20–28 ms, and the processor of the router uses up to 40% of its productivity.

Later, one of the users was changed to an intruder. Then the data transfer speed will reach the maximum value of 100 Mbit/s, the ping is 36-50 ms, and the loading of the router's processor reaches 100% of its productivity. Under such conditions, the bandwidth is redistributed in favor of the intruder. This, in turn, reduces the data transfer speed of the rest of the clients. There are also significant delays in data transmission of typical users, this leads to disconnections of the user, denial of access to remote resources [26-31].

That is, such a mode of operation of the equipment significantly reduces the quality of service for typical users. In cases where the tasks of routing open and closed network segments are performed by a single device (which is usually the case), overloading the router will lead to interruptions and deterioration of the performance of closed segments, although they are not directly affected by the prohibited effects.

The next step of the experiment was the implementation of the developed system for detecting outgoing malicious traffic in the researched environment (Figure 22).

In order to evaluate the effectiveness of the proposed system, we will conduct a study of its operation in different modes.

In the first version, we will consider the operation of the system with typical users, the absence of an intruder and a system for detecting malicious outgoing traffic. The performance indicators of the system are presented in Figure 23.

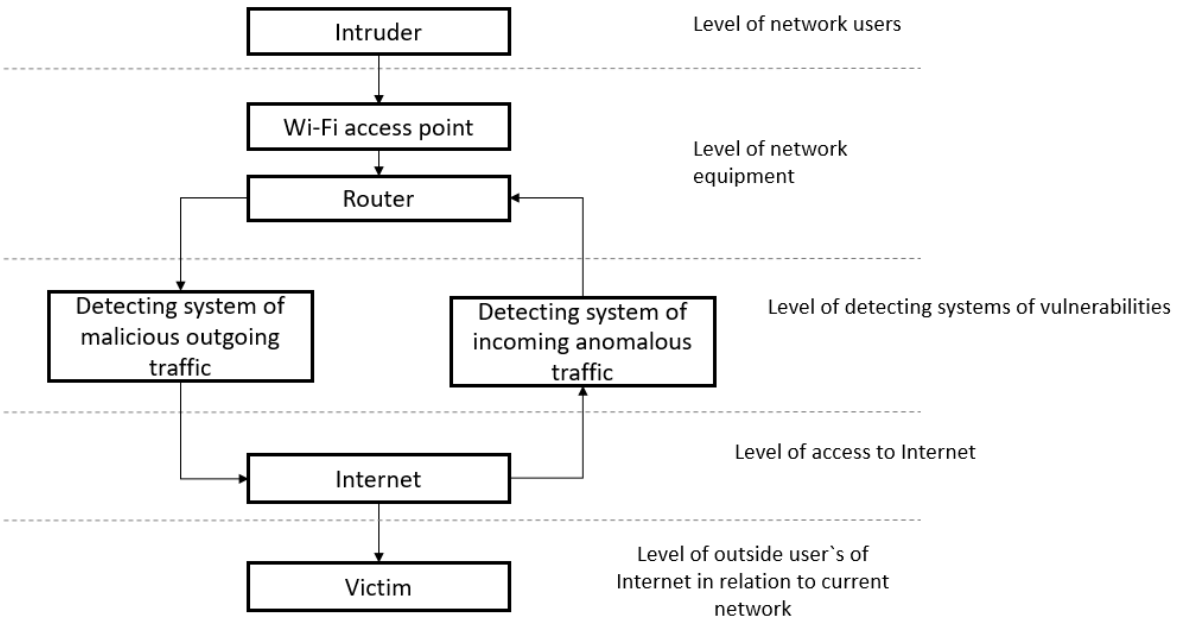

Figure 22: A network diagram using a detection system of malicious outgoing traffic

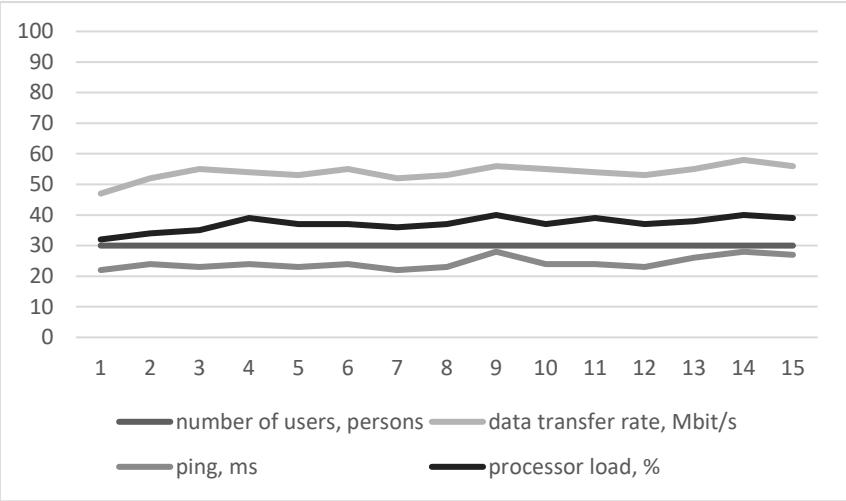

Figure 23: System operation diagram with typical users

In the second version, the operation of the system is presented with typical users and an intruder performing malicious actions, and the absence of a system for detecting malicious outgoing traffic. The performance indicators of the system are presented in Figure 24. The third version presents the operation of the system with typical users and an intruder performing malicious actions, with a system for detecting malicious outgoing traffic. The performance indicators of the system are presented in Figure 25. Looking at the diagrams, it can be concluded that the proposed system detects the intruder based on a previously known signature, while there is no noticeable increase in package transmission delays.

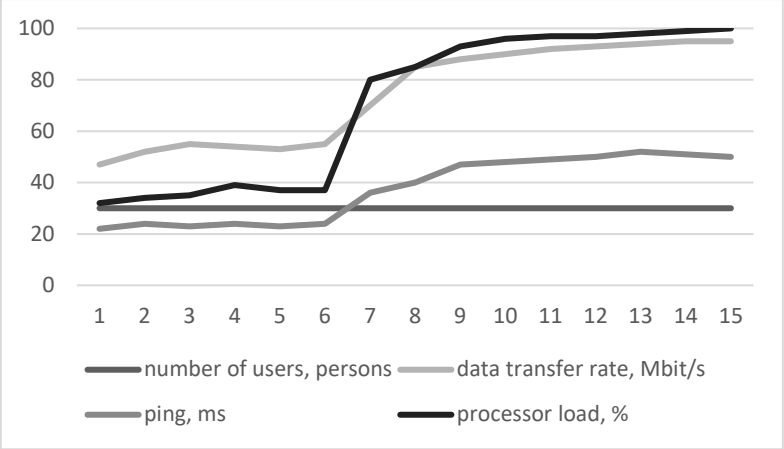

Figure 24: Diagram of system operation with typical users and an intruder performing malicious actions

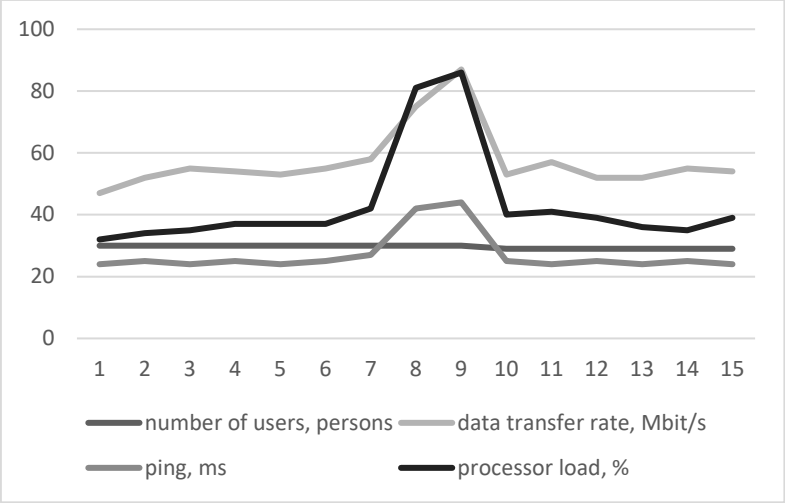

Figure 25: Diagram of the system operation with typical users and an intruder (performs malicious actions), a system for detecting malicious outgoing traffic

9. Conclusions

The article discusses ways to detecting malicious outgoing traffic to counter attacks and implement other threats in the public networks. A comparative analysis of methods for detecting malicious network traffic allowed us to come to a conclusion regarding their focus on protection against external influences. This is implemented through the analysis of incoming traffic. At the same time, little attention is paid to the analysis of outgoing traffic.

Studies have shown that quite often a network with a large number of users can itself become a threat to the network space. The reason can be both malicious actions of users and unintentional infection of network resources with malicious software. A significant potential for detecting malicious activity in the network lies in the control of outgoing traffic, an approach to the implementation of which based on signatures is proposed in the article.

An analysis of the work of the university's public network, which is characterized by a large number of users, a variety of used applications and the instability of user activity over time, is presented. Based on the results, a behavioral model of a legitimate user is proposed. Based on it, models behavior of the violator were developed and described during password attacks and denial-of-service attacks, when scanning the network, when setting up remote work, when trying to send spam. Models of behavior in the implementation of the specified harmful actions are reduced to a generalized model behavior of the violator.

The proposed models are used to determine features for analyzing outgoing traffic, build and

optimize a graph of the dependence of header elements on attack types. The principles of intrusion and the format of signatures are also detailed, and the rules for classifying signatures for identifying safe, malicious and undefined traffic are defined.

The analysis of signatures and determination of further actions is implemented by a hardware and software component, the algorithm of which works when implementing the proposed approach to detecting malicious outgoing traffic based on signatures is presented.

Experimental testing of the proposed approach proved its effectiveness for detecting the violator by signature dictionaries, while no noticeable increase in packet transmission delays is observed. Having a system to detect malicious outgoing traffic has benefits, including reducing the overall number of cyber attacks, preventing overloading of network equipment, and reducing the chances of compromising the current network and its owner.

Further improvement of the proposed approach requires determination of the principles of activation for obtaining signatures of unknown traffic and research of the system's response to other types of attacks that were not considered in the work.

10. References

[1] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans Emerging Tel Tech. 2021; 32:e4150. doi:https://doi.org/10.1002/ett.4150

[2] P. Radoglou-Grammatikis et al. Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Vol. 18, No. 3, March 2022, pp. 2041-2052.

[3] H.Sarjan, A. Ameli M. Ghafouri Cyber-security of industrial internet of things in electric power systems. IEEE Access, vol. 10, no. 92, pp. 92390-92409, 2022.

[4] A. S. A AL-Ghamdi, et al, Optimized Artificial Neural Network Techniques to Improve Cybersecurity of Higher Education Institution. Computers, Materials & Continua 2022, 72(2), 3385-3399. URL: https://techscience.com/cmc/v72n2/47241.

[5] M. Hijji, G. Alam. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors 22 (2022) 8663. doi: 10.3390/s22228663

[6] A.I.A. Alzahrani, M.Ayadi, M.M. Asiri, A.Al-Rasheed, A. Ksibi Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques. Electronics 11 (2022) 3665. doi: 10.3390/electronics11223665

[7] Y. Gao, H. Hasegawa, Y. Yamaguchi and H. Shimada Malware Detection by Control-Flow Graph Level Representation Learning With Graph Isomorphism Network. IEEE Access, 10 (2022) 111830-111841. doi: 10.1109/ACCESS.2022.3215267.

[8] A. Starke, K. Nagaraj, C. Ruben, N. Aljohani, S. Zou, A. Bretas, J. McNair, A. Zare Cross-layered Distributed Data-driven Framework for Enhanced Smart Grid Cyber-physical Security. IET Smart Grid 5 (2022) 1–19.

[9] A.S.Alqahtani, K.A. Abuhasel and M. Alquraish A Novel Decentralized Analytical Methodology for Cyber Physical Networks Attack Detection. Wireless Pers Commun 127 (2022) 1705–1716. doi: https://doi.org/10.1007/s11277-021-08716-5

[10] M. Shafiq, Z. Tian, A.K. Bashir, X. Du and M. GuizaniCorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021. doi: 10.1109/JIOT.2020.3002255.

[11] F. Louati, F.B. Ktata A deep learning-based multi-agent system for intrusion detection. SN Applied Sciences 2 (2020) 675. doi:https://doi.org/10.1007/s42452-020-2414-z

[12] S. Kim, S. Yoon and H. Lim Deep Reinforcement Learning-Based Traffic Sampling for Multiple Traffic Analyzers on Software-Defined Networks. in IEEE Access, vol. 9, pp. 47815-47827, 2021. doi: 10.1109/ACCESS.2021.3068459.

[13] S. Taheri, A.M.Bagirov, I. Gondal et al. Cyberattack triage using incremental clustering for intrusion detection systems. Int. J. Inf. Secur. 19 (2020) 597–607. doi: https://doi.org/10.1007/s10207-019-00478-3

[14] G. Rekha, S. Malik, A. K. Tyagi, M. M. Nair. Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security. Advances in Science, Technology and Engineering Systems Journal, 5 3 (2020) 72-81. doi: 10.25046/aj050310
[15] O.E. Elejla, M. Anbar, S. Hamouda, B. Belaton, T.A. Al-Amiedy, I.H. Hasbullah Flow-Based IDS Features Enrichment for ICMPv6-DDoS Attacks Detection. Symmetry, 14 (2022) 2556. doi: https://doi.org/10.3390/sym14122556
[16] V. Dzhedzhula, I. Yepifanova and Y. Kravchyk Use of the Theory of Fuzzy Sets in Determining the Level of Enterprise Security. 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 311-315, doi: 10.1109/ACIT54803.2022.9913150.
[17] X. Zhou, Y. Hu, W. Liang, J. Ma Q. Jin Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. in IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3469-3477, May 2021. doi: 10.1109/TII.2020.3022432.
[18] Y. Klots, V. Titova, N. Petliak, V. Cheshun, A.-B.M. Salem, Research of the Neural Network Module for Detecting Anomalies in Network Traffic. CEUR Workshop Proceedings, 3156 (2022) 378–389. URL: https://www.scopus.com/authid/detail.uri?authorId=57786856200
[19] A. Kanta, S. Coray, I. Coisel, M. Scanlon. How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts. Forensic Science International: Digital Investigation 37 (2021) 301186. doi:https://doi.org/10.1016/j.fsidi.2021.301186
[20] O. Pomorova, O. Savenko, S. Lysenko, A Kryshchuk, Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic, Communications in Computer and Information Science 370 (2013) 243-254.
[21] N. Z. M. Safar, N. Abdullah, H. Kamaludin, S. Abd Ishak, M. R. Mohd Isa. Characterising and detection of botnet in P2P network for UDP protocol. Indonesian Journal of Electrical Engineering and Computer Science 18 3 (2020) 1584-1595. doi: 10.11591/ijeecs.v18.i3.pp1584-1595
[22] M. Zipperle, F. Gottwalt, E. Chang, T. Dillon. Provenance-based Intrusion Detection Systems: A Survey. ACM Computing Surveys, 55 7 (2023) 135 1–36. doi: https://doi.org/10.1145/3539605
[23] MTProto Mobile Protocol. 2022. URL: https://core.telegram.org/mtproto
[24] Zoom network firewall or proxy server settings. 2022. URL: https://support.zoom.us/hc/en-us/articles/201362683-Zoom-network-firewall-or-proxy-server-settings
[25] Mahmud, Hasan, et al. What influences algorithmic decision-making? A systematic literature review on algorithm aversion. Technological Forecasting and Social Change 175 (2022): 121390.
[26] Lysenko S., Savenko O., Kryshchuk A., Klyots Y. Botnet detection technique for corporate area network / Savenko O., A. Kryshchuk, Y. Klyots. The IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Proceedings (Berlin, Germany, September 2013). Berlin, 2013. Vol. 1. Pp. 315-320.
[27] O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko, Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search, CEUR Workshop Proceedings 1844 (2017) 555–569
[28] Oksana Pomorova, Oleg Savenko, Sergii Lysenko, Andrii Nicheporuk. Metamorphic Viruses Detection Technique Based on the Modified Emulators. CEUR- WS, ISSN: 1613–0073 (Scopus). 2016. Vol. 1614. Pp. 375-383.
[29] Savenko O. Lysenko S., Kryschuk A. Multi-agent based approach of botnet detection in computer systems / Communications in Computer and Information Science. – 2012. – Vol. 291. – PP.171-180, ISSN: 1865-0929.
[30] L. Huang, H. Huang, J. Xiao and X. Lv, "Research on Adaptive Adjustment Method of Intelligent Traffic Light Based on Real-Time Traffic Flow Detection," 2022 5th International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, 2022, pp. 644-647, doi: 10.1109/ICAIBD55127.2022.9820545.
[31] S. K. Saini and M. Singh Ghumman, "Automated Traffic Management System Using Deep Learning Based Object Detection," 2022 International Conference on Machine Learning and Cybernetics (ICMLC), Japan, 2022, pp. 1-5, doi: 10.1109/ICMLC56445.2022.9941332.