Application of the Modified Irwin Method for Development of the Detecting DDOS-Attacks System

Andrey A. Tarasiev
IRIT-RTF; Ural Federal University named after the first President of Russia B.N.Yeltsin
Yekaterinburg, Russian Federation
andrew4800@mail.ru

Xenia D. Nisskhen
IRIT-RTF; Ural Federal University named after the first President of Russia B.N.Yeltsin
Yekaterinburg, Russian Federation
xenia.nisskhen@yandex.ru

Margarita E. Filippova
IRIT-RTF; Ural Federal University named after the first President of Russia B.N.Yeltsin
Yekaterinburg, Russian Federation
rituly_22@mail.ru

Elena F. Smoliy
Ural Federal University named after the first President of Russia B.N.Yeltsin
Yekaterinburg, Russian Federation
smoliylena@yandex.ru

Abstract

In this paper, we describe the development of a method for dynamically detecting DDoS-attacks in the initial stages. The method is based on the application of the modified Irwin method to identify the anomalous values of time series. At the same time, in order to eliminate or minimize the number of false positives, a method for further processing data on potentially abnormal values revealed using this method is proposed. The proposed method can be applied dynamically in real systems to monitor network traffic in real time. Also within the framework of the work a prototype of the system was developed, applying the described method on pre-assembled samples.

CEUR-WS.org/Vol-2298/paper9.pdf

1 Introduction

Modern people live in the digital age. An enormous role in the life of any member of modern society is played by information technology of varying complexity. Information exchange has reached such a level that many people do not imagine a different life. Undoubted contribution to this made the Internet.

To date, according to the research company Netcraft, there are about 1.7 billion Internet resources. Many organizations and people have their own web applications [1].

It is obvious that under such realities there can be a lot of problems related to maintaining the operability of these information systems. The range of problems can be very different - from information security problems associated with unauthorized access to data, to physical breakdowns of servers, network equipment or endpoints. One of the most common problems is the danger of DDoS-attacks.

As well-known popular victims of such attacks are commercial and information sites.

The purpose of the DDoS-attack is to block for some time access to the online resource by overloading the channel with "junk" requests, which inevitably leads to significant financial and other losses.

This type of attack is usually used for the purpose of extortion, damage to competitors, information wars, etc.

It is natural that with the increase in the number of Internet resources and the increased complexity and sophistication of information technology, the number of such attacks is growing significantly.

The situation is aggravated by the fact that almost anyone can organize a DDoS-attack today because the cost is not so high, contacts of performers can be found with the help of search services. Such availability and ease of organization of DDoS-attacks threaten almost any company that has ill-wishers.

According to the results of Kaspersky Lab's research, in 2017, every third Russian company (36%) was attacked at least once by a DDoS-attack. In 2016, there were half as many, only 17%. [2]

Despite this, many organizations, both commercial and independent, still do not consider them a serious threat. At the same time, inaccessibility of the site and failed transactions is only the tip of the iceberg. If in the case of hacking the system, intruders steal customer data and confidential information, then a DDoS-attack can result in the loss of important data, the reputation of the company, the outflow of existing customers or claims for services not provided.

It is also worth noting that the risk of being subjected to these attacks only continues to grow with time.

The aim of this work is to develop a method and a software tool designed to detect the onset of DDoS-attacks at the earliest stages. The use of such a tool can help in time to react to the onset attack and take appropriate measures with minimal damage.

2 Formulation of the problem

Currently, there are methods for dynamically analyzing network traffic, but most of them are internal closed development of individual companies. In other cases, these methods cannot detect the beginning of an attack on time and with high accuracy.

In many such systems, the control value of the allowed traffic for server requests is rigidly set. This value, as a rule, is revealed empirically and has a subjective character.

It is obvious that there can be two problems associated with the use of this approach - the response of the system to abnormal traffic may be too late, or false positives may occur.

The method being developed is designed to solve these problems.

In the framework of this task, the following definition will have adopted: the attack consists of a sharp anomalous increase in requests to the server, and, as a consequence, incoming packets.

Thus, dynamic traffic analysis requires tracking of abnormal peaks.

For the research, the real impersonal data from the company's database hosting provider was used. This data includes information about traffic that has passed through certain vendors to the company's IP addresses. IP addresses are divided into subnets.

In this case, the data is represented as the average traffic value and the number of packets on subnets and IP addresses in equal intervals set every 5 minutes.

The main objective of the method is to identify by a dynamic analysis of the data a specific five-minute interval of the beginning of the attack and find out which subnet was attacked. After an attack is detected on any subnet should be search for the specific IP address being attacked.

It should be noted that the simplification associated with the use of averaged values in given time intervals is associated with the technical features of the systems used in the research. It is assumed that the developed method will also work adequately with non-averaged data.

It is expected that the use of this system will significantly reduce the potential damage from hacker attacks, by providing the ability to react quickly to the acute situation in the early stages.

3 Method definition

Based on the initial data on the passing traffic, it is possible to construct a visual diagram of the time series. Let's imagine it as the dependence of the number of input packets on time.

As already mentioned, the DDoS-attack on such a graph will be clearly visible in the form of a peak, due to sharply growing abnormal traffic.

Thus, we can assume that it is sufficient to use any method of identifying local maxima. However, this statement would be incorrect, since not every local extremum can be considered an anomaly.

An example of such a situation is shown in the following figure (Figure 1).

The given schedule is constructed on the basis of the presented sample according to the monitoring of traffic of one subnet for a specific day – April 23, 2018.

With the naked eye, it can be seen that on this chart without averaging there is a large number of local extremes, which in this case are not anomalous.

In this time series, a fairly high but stable load of network traffic in the subnet is observed. However, there is no attack in this case, however, the proposed method would produce a large number of false positives. This is due to the fact that not every splash can be a DDOS-attack. High traffic of the activity of users of the resource can be associated with an external event, for example, the seasonality of sales, etc.

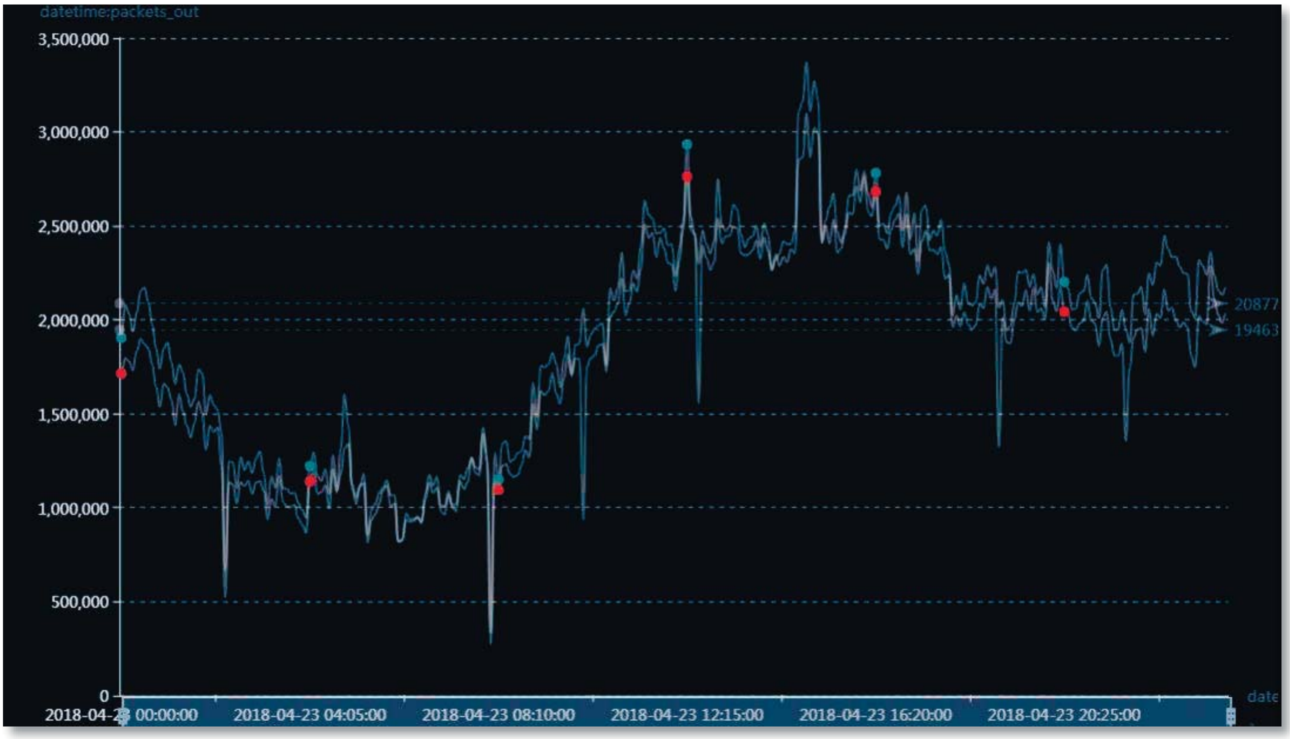


Figure 1: The graph of the average number of incoming packets per time interval over a single subnet.

Thus, it is necessary to apply a method that could filter out false positives. To achieve this the modified Irwin method proposed for the analysis of electromagnetic radiation was used [3].

This method allows one to effectively separate the anomalous peaks of the time series from the background ones.

The following method consists in calculating the coefficient for each considered interval based on the standard deviation and the mean amplitude value. The calculated value of λ is compared with the tabulated value, which leads to the conclusion that there is an anomaly. If any value of the calculated coefficients λ is greater than the tabulated one, then the corresponding value of the level of the series, in our case the number of transmitted packets, is considered as anomalous [3, 4].

As a result, for similar peak values of the number of packets presented by this method, false triggering was eliminated and attacks were detected, even in cases when they were artificially smoothed (Figure 2).

However, for a number of other situations, this method still did not work out correctly. This is due to the fact that the anomalies are difficult to track in the early stages with a stable high load. Thus, some bursts of activity cannot be tracked by the proposed method.

However, in the context of processing network traffic, additional criteria can be introduced that minimize the number of errors.

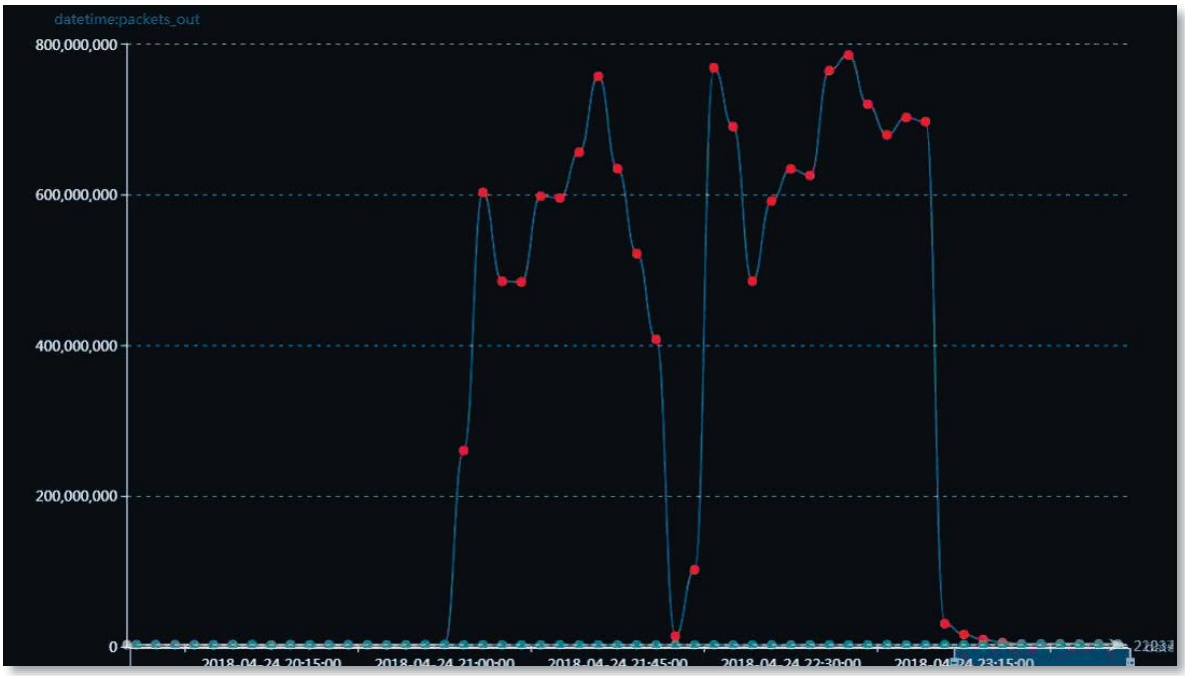


Figure 2: The graph of the average number of incoming packets per time interval over a single subnet.

As a result of the analysis of network traffic, a new modification of the Irwin method [3] was proposed. This modification focused specifically on monitoring network traffic. The new method consists in the subsequent processing of suspicious cases found using the basic modifications of the method of searching for abnormal extrema.

As the main among the new selection criteria, the ratio of incoming and outgoing traffic was chosen. By an experimental analysis of the ratio of the number of input and output packets, the following variants were identified:

1. If incoming traffic decreases and the input traffic increases, then this interval is not considered suspicious, since there is no attack on incoming traffic (Figure 3).

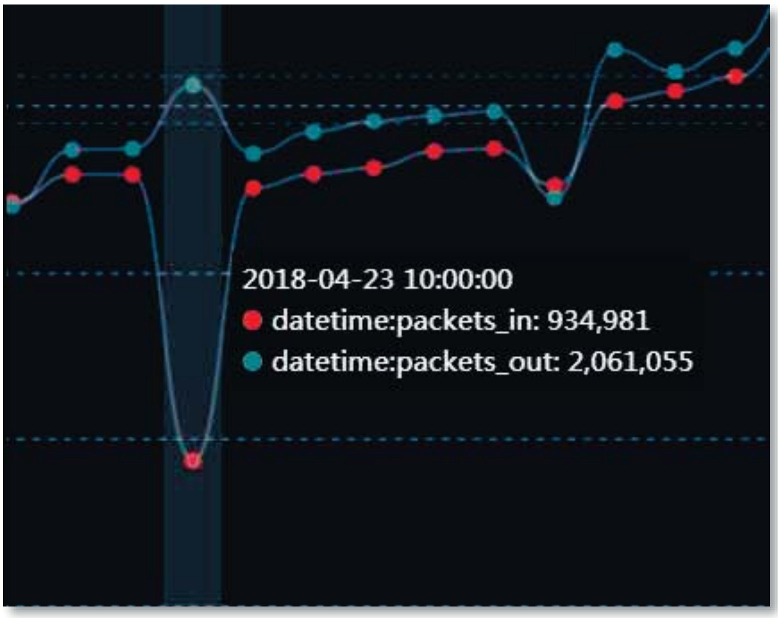


Figure 3: The discrepancy between the input and output traffic

2. If both traffic changes equally or in proportion, then this is most likely a natural load associated with the inflow or outflow of real users of the system due to some external causes (Figure 4).

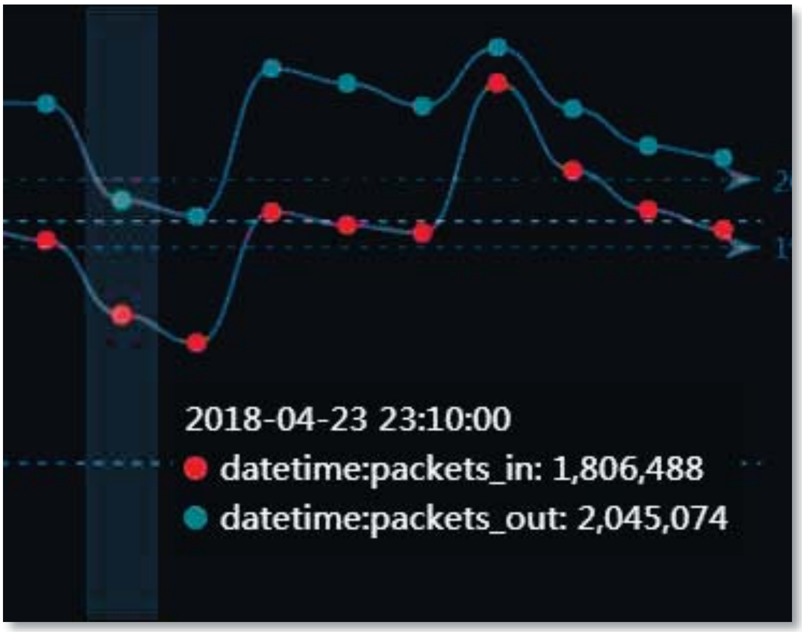


Figure 4: The proportional change in input and output traffic

3. Similarly, if incoming traffic is insignificantly higher than the outgoing traffic, then this is also not a pronounced attack. These leaps are most natural and common. A sharp anomalous activity peak will be detected directly by the Irwin method at the next nearest time intervals (Figure 5).
4. If incoming traffic significantly increased compared to outgoing traffic, then this is an explicit DDOS-attack.
5. Likewise, if incoming traffic increases dramatically and the outgoing traffic decreases – this may indicate that the attack has been going on for some time.

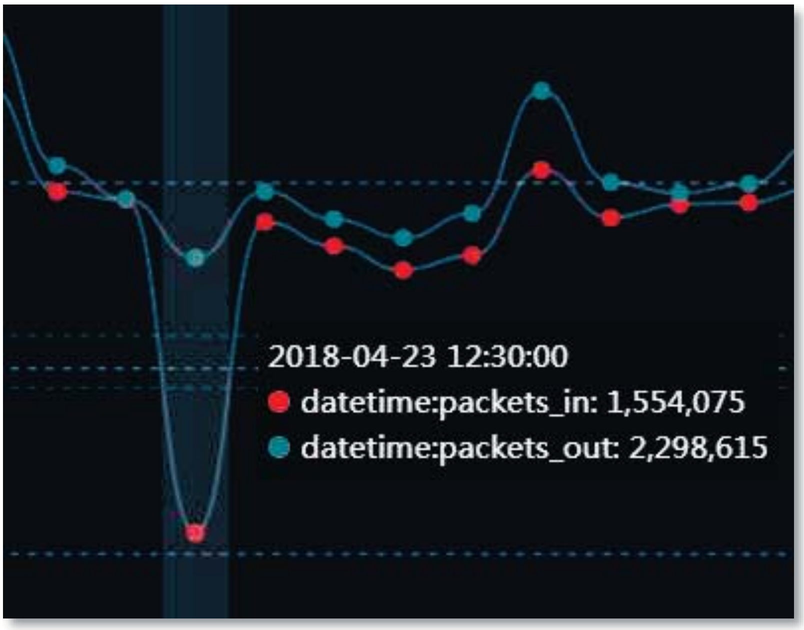


Figure 5: Insignificant growth of input traffic relative to the output

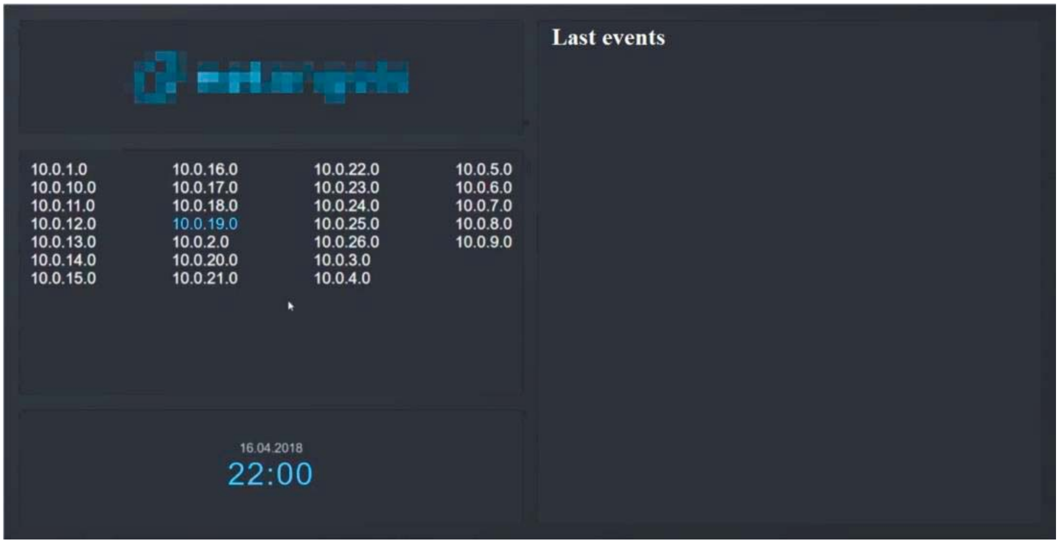
Thus, the algorithm for determining the time interval for a potential attack on a subnet is as follows:

1. Using the modified Irwin method [3], local extrema of the function of the dependence of the number of incoming packets on the subnet are detected, which are suspicious for the presence of an anomalous increase in the value. In this case the subnet is marked as potentially attacked.
2. Then the subsequent processing of the detected values occurs. Input traffic is compared with the output in the same time intervals on the basis of which there is a filtering of suspicious values from false positives of the method.
3. In the event that, as a result of the processing, the anomalous traffic values remain, the subnet is analyzed deeper for the detected time intervals. At this stage, the specific attacked addresses are searched for.

Based on the developed algorithm, a prototype of the monitoring information system was designed and developed.

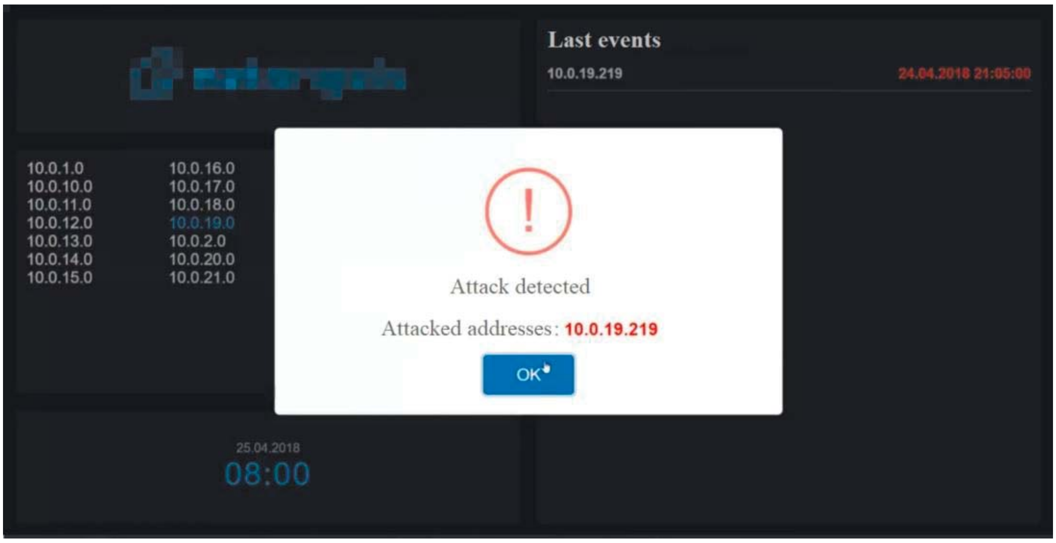
4 Proposed solution

In the course of the work, a software system was developed, the interface of which is presented in the form of a dashboard (Figures 6-7) [5,6].



10.0.1.0
10.0.10.0
10.0.11.0
10.0.12.0
10.0.13.0
10.0.14.0
10.0.15.0
10.0.16.0
10.0.17.0
10.0.18.0
10.0.19.0
10.0.2.0
10.0.20.0
10.0.21.0
10.0.22.0
10.0.23.0
10.0.24.0
10.0.25.0
10.0.26.0
10.0.3.0
10.0.4.0
10.0.5.0
10.0.6.0
10.0.7.0
10.0.8.0
10.0.9.0

Figure 6: The system prototype interface



10.0.19.219 24.04.2018 21:05:00

10.0.1.0
10.0.10.0
10.0.11.0
10.0.12.0
10.0.13.0
10.0.14.0
10.0.15.0
10.0.16.0
10.0.17.0
10.0.18.0
10.0.19.0
10.0.2.0
10.0.20.0
10.0.21.0

Attack detected

Attacked addresses: 10.0.19.219

Figure 7: Visualization of the detected attack in the system prototype interface

The work process of the system can be described as follows. First, the data on subnets is analyzed automatically.

The analysis is performed using a modified Irwin method for detecting anomalous bursts of time series levels.

When a potential anomaly is detected, the time of a possible attack on the subnet is fixed, after which the system begins a detailed analysis of the IP addresses in that subnet at this point in time.

After analyzing the suspicious IP-addresses, it is calculated from which of them this attack occurred, after which the information is recorded in the log and displayed in the dashboard.

5 Conclusion

Thus, within the framework of the work done, a basic study of the method of dynamic detection of DDoS-attacks in real time at the initial stages was carried out. This method is based on the application of the modified Irvine method to determine the anomalous values of the local extrema of the function.

During the analysis of the admissibility of using this method in monitoring network traffic, it was decided to modify the algorithm for applying this method by secondary processing of the results of calculations in order to eliminate or minimize the number of false positives.

The proposed method can be applied dynamically in real systems to monitor network traffic in real time.

In addition, within the framework of the work, a prototype of the system was developed that applies the described method to pre-assembled samples of subnets traffic values. The values of the number of packets were measured with an interval of 5 minutes.

It is expected that this method can also adequately work in real time with data collected at shorter time intervals.

The application of this system will significantly reduce the potential damage from hacker attacks, by providing the ability to react quickly to an acute situation in the early stages.

5.1.1 Acknowledgements

The work was supported by Act 211 Government of the Russian Federation, contract № 02.A03.21.0006.

6 References

1. Netcraft official site. Available at: https://news.netcraft.com/. (Accessed 10 august 2018)

2. Kaspersky Lab's official site. Available at: https://www.kaspersky.ru/. (Accessed 5 may 2018) (in Russian)

3. S.V. Trofimenko, S.V. Trofimenko, A.Y. Marshalov, N.N. Grib, I.I. Kolodeznikov. Modifikacija metoda Irvina dlja vyjavlenija anomal"nyh urovnej vremennyh rjadov: metodika i chislennye jeksperimenty [Modification of the Method for Irwin detect abnorval levels time series: Method and Numerical Experiments].Sovremennye problemy nauki i obrazovanija, {255, October 2014, (5). (in Russian)

4. Irwin method tabulated values. Available at: http://arhiuch.ru/st7.html. (Accessed 6 may 2018) (in Russian).

5. I. A. Spitsina, K. A. Aksenov. Multiagent method of analysis and synthesis of information systems {Ekaterinburg, 2017

6. K. A. Aksyonov, E. A. Bykov, O. P. Aksyonova. Development and application of software engineering solution BPsim.SD. Proceedings - UKSim-AMSS 7th European Modelling Symposium on Computer Modelling and Simulation, 321-325 {November 2013.