Development Of A Method For Detecting Deviations In The Nature Of Traffic From The Elements Of The Communication Network

Oleksandr Laptiev [1], Nataliia Lukova-Chuiko [2], Serhii Laptiev [3], Tetiana Laptieva [4], Vitaliy Savchenko [2], Serhii Yevseiev [3]

[1 2 3 4]*Taras Shevchenko National University of Kyiv, 24 Bogdana Gavrilishina str., Kyiv, 04116,Ukraine,*
[2]*State University of Telecommunications, 7 Solomenska str., Kyiv, 03110, Ukraine*
[3]*Simon Kuznets Kharkiv National University of Economics, 9-A Nauky ave., Kharkiv, 61166,Ukraine,*

Abstract

The article presents an analysis that showed the lack of scientific and methodological apparatus, universal devices or automated software packages to ensure the prompt implementation of traffic analysis and information transfer to automated systems or relevant specialists.

A new developed method is proposed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The developed method allows to carry out operative (real-time) informing of responsible specialists, or transfer of necessary data to the automated complex, about deviation of character of traffic from network elements (separate telephone numbers, number capacities, trunk groups, etc.) which is fixed in primary data. Deviations, the nature of traffic from the elements of network parameters are measured from the usual traffic of the telephone network relative to these elements.

This method has a methodology that takes into account practical recommendations for constant coefficients, calculations. These coefficients are selected by calculation and empirical. This reduces the response of the system using the developed technique to the deviation of the communication parameters.

Keywords

traffic deviation, coefficient, model, telecommunication networks, primary data, communication.

1. Introduction

According to the latest research by the World Association for the Control of Telecommunication Network Violations (CFCA), in 2017 the losses from violations in the telecommunications industry amounted to 74.4-90 billion. This is approximately 57% more than the figure obtained in CFCA studies three years ago [1]. Violations on telecommunications networks are actions of subscribers, telecommunications operators or third parties that are aimed at obtaining telecommunications services at a lower rate or without payment. CFCA experts count about 200 types of violations on telecommunications

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: alaptev64@ukr.net (A. 1); lukova@ukr.net (A. 2); salaptiev@gmail.com (A. 3); savitan@ukr.net (A. 4); tetiana1986@ukr.net (A. 5); serhii.yevseiev@hneu.net (A. 6)
ORCID: 0000-0002-4194-402X (A. 1); 0000-0003-3224-4061 (A. 2); 0000-0002-7291-1829 (A. 3); 0000-0002-3014-131X (A. 4); 0000-0002-5223-9078 (A. 5); 0000-0003-1647-6444 (A. 6)
© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-3200/paper1.pdf

networks. The most common violations by subscribers are third-party connection to the subscriber line in order to receive free telematics services «900», the implementation of long-term international calls, the organization of unauthorized negotiation points [2, 3]. It is a violation on the part of third parties to use hardware and software to obtain international traffic from the Internet and complete it on a public telecommunications network under the guise of.

local, which leads to interference in the work of communications, substitution of call information. On the part of operators, the most common is the unauthorized, without relevant agreements, termination of incoming long-distance and international traffic to the public network under the guise of local. Abuses lead to loss of revenue, subscriber complaints and disruption of telecommunications networks.

The fight against abuse on telecommunications networks is largely based on the analysis of data on services and data contained in payment systems with subscribers and operators [4, 5-7]. Detection of suspicious actions of subscribers and their analysis is the main principle of modern systems of protection against violations (Fraud Management System, FMS). The key criteria for FMS efficiency are speed of operation, flexibility of debugging algorithms that provide incident detection and analysis, and the availability of standardized interfaces for integration with billing platforms and the Customer Relationship Management System (CRM).

1.1 Literature analysis and problem statement

A significant number of publications are devoted to the task of ensuring the prompt implementation of the analysis of communication traffic.

Thus, in [8] considers the analysis of communication traffic with different technical parameters, which unites only one thing - they can only show and (at best) store panoramas of signals in the communication network. They do not solve the problem of communication traffic analysis at all.

The article [9,10] presents the results of the study of SS7 network security. The Signaling System 7 standard is used to exchange service information between network devices in telecommunications networks. At the time this standard was being developed, only fixed line operators had access to the SS7 network, so security was not a priority. Today, the signaling network is no longer as isolated, so an attacker, who in one way or another gained access to it, has the opportunity to exploit security vulnerabilities in order to listen to voice calls, read SMS, steal money from accounts, bypass billing systems or affect the operation of the mobile network. However, no real protection is offered.

In [11-14] the development of mobile communication over the last decade is considered. It is noted that there has been huge progress in the field of wireless communications and especially in the field of 4G cellular networks. However, it will take several years to fully switch to 4G systems, and work has already begun on 5G technologies and their problems. Network security issues are not addressed.

In [15,16] it is said that the effective work of employees is one of the main conditions for the company's success. Uncontrolled access of employees to the Internet can be a serious obstacle to this. Without proper control, an average of up to a third of working time can be spent visiting non-work-related resources. That is why it is important to set up Internet traffic control and use a traffic counter. Protection and proper control over mobile telephone communication has not been properly considered and described [17].

Thus, the most critical for the operator are: violation of the routing of long-distance and international calls, detection of subscriber numbers on outgoing local traffic, activity of operators on incoming local traffic, similar to the operation of gateways to complete incoming long-distance and international traffic, detection of changes in activity of subscriber numbers, which may be evidence of third-party connection to the subscriber line or actions of the subscriber that potentially lead to complaints, non-payment for services and debt write-off. Automated analysis of data on services must be operational.

From the analysis of modern literature it can be concluded that there are almost no universal devices or automated software to ensure the rapid implementation of traffic analysis and information transmission by automated systems or relevant specialists. Therefore, the topic of developing a method designed to ensure the rapid implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists, the method of informing

responsible professionals is relevant and very important.

Thus, the development of a method designed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists, the method of informing responsible professionals is very relevant.

2. The material and methods

The operation of violation detection mechanisms is based on the processing of records of network-registered CDR events (Call Detail Record). The anti-fraud system looks for non-compliance with certain conditions or non-compliance with a given pattern, the characteristics of the subscriber's behavior. When the detection module finds one of the anomalies, it generates a warning message.

Typical conditional checks for FMS systems include:

1. Non-existent numbering (calling party number «A»)
2. Verification of authorization, temporary blocking of number «A»
3. Correspondence to the set template
4. Checking the «black and white lists»
5. Frequently repeated subscriber numbers «A» or «B»
6. Check the connection duration
7. Verification of suspicious calls from «A» subscribers for inclusion in the list of «B» subscribers who most often receive calls from abroad.
8. Changes in the intensity of signal and information load.

The search for a given template is based on traffic patterns that are created for each telecommunications operator. The difference between the existing signal and information traffic and the template indicates a possible violation. An additional use of templates is to compile a profile of the subscriber (telecommunications operator) of the attacker and search for compliance with such a profile among existing subscribers (telecommunications operators). Profiles can contain such characteristics as:

- activity during the day;
- activity in the evening;
- activity at night;
- volumes of outgoing traffic to mobile phones;
- volumes of outgoing traffic to fixed local numbers (including frequently used numbers);
- volumes of outgoing traffic to fixed numbers in other cities (including frequently used numbers);
- volumes of outgoing traffic to fixed numbers in other countries (including frequently used numbers);
- number range of the operator;
- average number of connections over time;
- average amount of traffic over time;
- average connection duration;
- number of unique numbers;
- characteristic directions.

The most critical for the Customer in terms of reducing revenue loss are: violation of the routing of long-distance and international calls, detection of subscriber numbers on outgoing local traffic, activity of operators on incoming local traffic, similar to the operation of gateways to complete incoming long-distance and international traffic in the activity of subscriber numbers, which may be evidence of third-party connection to the subscriber line or actions of the subscriber that potentially lead to complaints, non-payment for services and debt write-off. Automated analysis of data on services must be operational. Thus, at this stage it is important to develop a method designed to analyze traffic and inform about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The main tasks in developing the method will be:

1. Debugging the elements of the telecommunications network. Automatic or with the participation of the operator
2. Providing automatic analysis, data classification, search for deviations of behavior of elements of a telecommunication network from a usual profile.
3. Creation of an detection algorithm based on the features of violations that create a dynamic over time impact on the network, causing anomalous phenomena.
4. Development of a graphical display of changes in quantitative characteristics over a period of time.
5. Estimation of conformity of parameters of anomalies (non-existent number, big duration of a call, etc.) to the values characteristic of this type.
6. Assessment of anomalies on the degree of probability of violation to determine the priority of response.
7. Development of information on the detection of deviations and events.

8. Development of a user-friendly operator interface.

Block detection scheme, which is based on the characteristics of violations, it is possible to present in Figure 1.

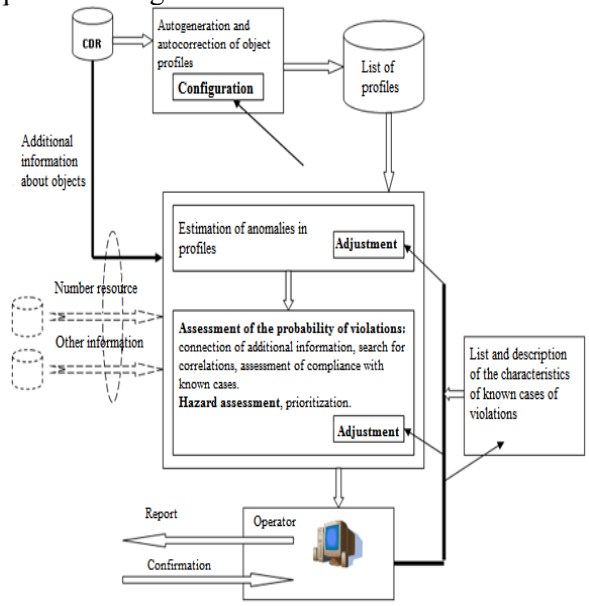

Figure 1: Block diagram of detection of estimates of profile anomalies for detection of violations

To assess the quantitative characteristics of the object and the dynamics of changes over time, it is proposed to use the method of exponential averages with different smoothing coefficients:

$$Q_t = (1-k)Q_{t-\Delta t} + kq_{\Delta t}, \qquad (1)$$

where:

Q is the exponential average value;

q - new dimension;

k is the smoothing coefficient;

Δt - interval between measurements;

The formula uses a constant interval of measurements. The profile correction for each call is complex, because in this case the smoothing factor is a complex exponential function of the measurement interval. However, the features of the parameters allow the use of simpler formulas.

The optimal number of average values and values of smoothing coefficients for each parameter can be obtained experimentally. To begin with, it is assumed to use for each parameter three values with coefficients k = 0.3; 0.05 and 0.005 with a focus on the daily interval of measurements.

For all the parameters and coefficients used below, the values that can be used in the development are presented, but when obtaining practical results, these values can be changed by the operator. In addition, the use of some profile parameters and anomaly calculations may be impossible or impractical, and others may need to be added.

Traffic will be estimated as the average daily number of seconds of connections:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \qquad (2)$$
$$\text{if } \Delta t < 86400$$

And

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \qquad (3)$$
$$\text{if } \Delta t \geq 86400$$

where:

T is the duration of connections in seconds;

Δt - time between the ends (beginnings) of the previous and new call in seconds.

The following types of traffic are provided for analysis:

- local outgoing
- long distance outgoing
- international outgoing
- input

We suggest estimating the intensity of the call flow as the average daily number of connection attempts:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT,\ \Delta t < 86400 \qquad (4)$$

And

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{if } \Delta t \geq 86400 \qquad (5)$$

where:

T is the duration of connections in seconds;

Δt - time by the ends (beginnings) of the previous and new call in seconds.

It is estimated the intensity of the flow of calls:

- incoming
- outgoing
- effective.

The distribution of traffic by time type is estimated as the average daily number of seconds of connections for working time.

- working hours - 1st-5th day of the week from 8-30 to 17-30;

- non-working hours - 1st-5th day of the week from 0-00 to 8-30 and from 17-30 to 24-00;

- 6th-7th day of the week from 0-00 to 24-00.

The distribution of traffic by time of day will be estimated as the average daily number of seconds of connections during the day.

- daytime from 7-00 to 24-00;

- night time from 0-00 to 7-00.

Signal traffic is estimated as the average number of bytes of signal information per call:

$$Q_t = (1-k)Q_{t-\Delta t} + kB, \quad (6)$$

where:

B is the number of bytes of signal information in the call.

The instability of stable network parameters of the object is estimated by their change from call to call. One characteristic can be used for all parameters.

For each call:

$$Q_t = LQ_{n-1} + \sum h_i, \quad (7)$$

where:

hi - increment levels for parameters whose values differ in previous and subsequent calls;

L is a factor that takes into account outdated information L = 0.9.

Other parameter values (if present in the CDR):

- access (ISDN, non ISDN) h = 10;

- category of the subscriber calling h = 5;

- the presence or absence of signaling interaction when establishing a connection h = 8;

- invalid localization of the calling subscriber (correspondence of the address to the admissible template) h = 200;

- invalid subscriber category that causes h = 100.

It is necessary to provide for the possibility of expanding and changing similar parameters in the future, as well as the use of different characteristics for different groups of parameters.

Additional coefficients:

- is a constant additional factor that allows you to reduce or increase the sensitivity to anomalies in the assessment. Can only be changed by the operator;

- is a temporary additional factor that reduces or increases the sensitivity to anomalies in the assessment. It can be changed only by the operator, but then automatically strive for a normal value.

After each call, a temporary additional factor is determined by:

$$K2_t = (1-k)K2_{t-\Delta t} + kK2_{norm} \quad (8)$$

where:

Δt - time between the ends (beginnings) of the previous and next calls in seconds;

K2norm is the normal value;

k is the smoothing coefficient, k = 0,05.

Normal values for additional coefficients: K1norm = 100, K2norm = 100.

We will evaluate the anomalous behavior of the object by the following method:

The anomaly in the behavior of the object is assessed by the overall rating, as the average of the identified anomaly, taking into account additional coefficients.

$$A_{pr} = \frac{(\sum A) * K1 * K2}{(\sum C) * K1_{norm} * K2_{norm}}. \quad (9)$$

K1 - constant additional coefficient;

K2 - temporary additional coefficient.

When creating an object, the field T starts the time of the beginning of the observation, in the field K2 - a reduced value to stabilize the characteristics, in other fields - the default values.

To determine the anomalies, use the following method:

When determining anomalies, the coefficients and parameters common to all objects are used:

C - weighting factor, taking into account the impact of each anomaly on the overall rating;

m is a parameter that compensates for the high uncertainty in the profiles of low-traffic objects.

Traffic (A1, A2, A3, A4):

$$A(0.3) = C(0.3) * \frac{|Q(0.3) - Q(0.05)}{Q(0.05) + m}, \quad (10)$$

$$A(0.05) = C(0.05) \frac{Q(0.05) - Q(0.005)}{Q(0.05) + m}.$$

To determine the anomalies you need to set the traffic parameters, set the common for all objects coefficients and parameters of table 1 and table 2:

Table 1

Given the weights of anomalies

$C_1(0.3)$	$C_1(0.05)$	$C_2(0.3)$	$C_2(0.05)$
1	3	20	60

Table 2.

The specified parameters for determining anomalies

m_1	m_2	m_3	m_4
200	100	80	200

The connection duration will be calculated as follows:

Outgoing traffic:

$$Q_{tout} = Q_1 + Q_2 + Q_3; m_{tout} = m_1 + m_2 + m_3 \quad (11)$$

Outgoing calls

$$A5(0.3) = C5(0.3) * \left[\left| \frac{(Q_{Tout}(0.3) + m_{Tout}) * (Q5(0.05) + m_5)}{(Q5(0.3) + m_5) * (Q_{Tout}(0.05) + m_{Tout})} - 1 \right| \right] \quad (12)$$

$$A5(0.05) = C5(0.05) * \left[\left| \frac{(Q_{Tout}(0.05) + m_{Tout}) * (Q5(0.005) + m_5)}{(Q5(0.05) + m_5) * (Q_{Tout}(0.005) + m_{Tout})} - 1 \right| \right] \quad (13)$$

Incoming calls

$$A6(0.3) = C6(0.3) * \left[\left| \frac{(Q4(0.3) + m_4) * (Q6(0.05) + m_6)}{(Q6(0.3) + m_6) * (Q4(0.05) + m_4)} - 1 \right| \right] \quad (14)$$

$$A6(0.05) = C6(0.05) * \left[\left| \frac{(Q4(0.05) + m_4) * (Q6(0.005) + m_6)}{(Q6(0.05) + m_6) * (Q_4(0.005) + m_4)} - 1 \right| \right] \quad (15)$$

To determine the duration of the connection, you need to specify the traffic parameters, according to the developed method, the coefficients common to all objects and the parameters are given in table 3:

Table 3

Connection duration settings are set

C_5 (0.3)	C_5 (0.05)	C_6 (0.3)	C_6 (0.05)	m_5 (0.3)	m_6 (0.05)
3	10	3	10	5	5

According to the developed method, we will determine the effectiveness:

Total calls:

$$A7(0.3) = C7(0.3) * \left[\left| \frac{Q7(0.3) + 0.45 * m_{Nall}}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} \right| \right] \quad (16)$$

$$A7(0.05) = C7(0.05) * \left[\left| \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q7(0.005) + 0.45 * m_{Nall}}{Q_{Nall}(0.005) + m_{Nall}} \right| \right] \quad (17)$$

Where C7 (0.3) = 3 and C10 (0.05) = 10

The section by time type will be performed as follows:

Total traffic:

$$A8(0.3) = C8(0.3) * \left[\left| \frac{Q_{Tall}(0.3) - k_1(d,h) * Q8(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right| \right] \quad (18)$$

k1(d, h), k2(d) - coefficients that take into account the error of exponential averaging (d - day of the week, h - hour);

The coefficients that take into account the error of exponential averaging are given in table 4 and table 5.

Table 4

Error coefficients of exponential averaging d=1,2,3

h	$k_1(d,h)$	h	$k_1(d,h)$	h	$k_1(d,h)$
0	1.470	0	1.151	0	0.992
1	1.489	1	1.165	1	1.004
2	1.507	2	1.180	2	1.017
3	1.527	3	1.195	3	1.030
4	1.546	4	1.210	4	1.043
5	1.565	5	1.226	5	1.056
6	1.585	6	1.241	6	1.069
7	1.605	7	1.257	7	1.083
8	1.626	8	1.273	8	1.097
9	1.529	9	1.216	9	1.056
10	1.444	10	1.164	10	1.018
11	1.369	11	1.117	11	0.984
12	1.302	12	1.075	12	0.952
13	1.242	13	1.036	13	0.923
14	1.188	14	1.100	14	0.895
15	1.139	15	0967	15	0.870

Table 5

Error coefficients of exponential averaging

d	1	2	3	4
$k_2(d)$	1.031	1.008	0.988	0.970

$$A8(0.05) = C8(0.05) * \left[\left| \frac{Q_{tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{tall}(0.05) + m_{tall}} - \frac{Q_{tall}(0.005) - Q8(0.005)}{Q_{tall}(0.005) + m_{tall}} \right| \right] \quad (19)$$

where C8(0.3)=5 and C8(0.05)=15

The distribution of time of day we calculate by the expression:

$$A9(0.3) = C9(0.3) * \left[\frac{Q_{Tall}(0.3) - k_3(h) * Q9(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right] \quad (20)$$

$$A9(0.05) = C9(0.05) * \left[\frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.005)}{Q_{Tall}(0.005) + m_{Tall}} \right] \quad (21)$$

where:

k3(h) - coefficient that takes into account the error of exponential averaging (h - hour);

Table 6

The error rate of exponential averaging

h	0	1	2	3
$k_3(h)$	0.9709	0.9832	0.9956	1.0082

h	8	9	10	11
$k_3(h)$	1.0347	1.0288	1.0230	1.0173

h	14	15	16	17
$k_3(h)$	1.0012	0.9960	0.9910	0.9861

For the developed technique C9 (0.3) = 8; C9 (0.05) = 24.

We will define signal traffic by expressions:

$$A10(0.3) = C10(0.3) * \left[\frac{Q10(0.3)}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} \right] \quad (22)$$

$$A10(0.05) = C10(0.05) * \left[\frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q10(0.005)}{Q_{Nall}(0.005) + m_{Nall}} \right] \quad (23)$$

Coefficient C10 (0.3) = 20, coefficient C10 (0.05) = 60

The stability of the network parameter will be determined by the expression

$$A_{11} = W \quad (24)$$

Not all objects can be further processed, but only objects with the highest overall anomaly rating. It is enough to process about 1% of the total.

The assessment of the probability of violation, in contrast to existing methods, will be determined taking into account additional factors. In addition to the high level of anomaly of the object profile, additional factors that increase the possibility of detecting fraud in the assessment are:

- correlation of events of anomalous objects - coincidence of unique addresses in records of calls of objects for the last time (2-3 days);

- compliance of the profile of the object of the known case of violation, the coincidence of specific for this known case information about the call (direction, addressing) recently;

- inconsistency of the object profile with the typical subscriber accounting profile. (It is possible only if there is access to the subscriber accounting database, not necessarily in the early stages of development, but it is necessary to provide for such a possibility in the future).

Determining the probability of violation

$$P = MAX\left(\frac{A}{A+a} MAX(P_{known}) P_{subbase}\right) \quad (25)$$

where:

$\frac{A}{A+a}$ - the probability of violation, determined by the anomaly of behavior;

a - anomaly at 50% probability. The value of a can be obtained experimentally.

First you can use: a = 20;

$$A = A_{pr} + \sum A_{cor.pr.} \quad (26)$$

where:

Acor.pr - anomaly of the object, which has a correlation in the calls (when checking it is necessary to exclude coincidence at popular addresses: special services, serial modem pools, etc.), if the correlation is not defined - *Acor.pr=0*;

Psubbase - the probability of fraud, which is estimated by the inconsistency of the object profile to the typical profile in accordance with the subscriber accounting.

Pknown - the probability of a known type of violation (determined for each known type). The method of determining the probability of a known type of violation can also be based on the correspondence of characteristic anomalies in the profile of the observed object and the profile of the violating object at the time of detection, as well as correlations in calls by addresses

or prefixes. More precisely, the method can be determined only after the accumulation of a sufficient number of experimental results.

The assessment of the degree of risk of fraud according to the developed methodology will be calculated as follows.

Assessment of the degree of danger is necessary for cases that require priority intervention. They

can be considered as the effect of the probability of violation on loss or unearned income:

$$\Delta Q(0.3) = | Q(0.3) - Q(0.05) | \quad (27)$$

$$\Delta Q(0.05) = | Q(0.05) - Q(0.005) | \quad (28)$$

$$D = P * \begin{pmatrix} \Delta Q1(0.3) + k_2 * \Delta Q2(0.3) + k_3 * \Delta Q3(0.3) + \\ + L * (\Delta Q1(0.05) + k_2 * \Delta Q2(0.05) \\ + k_3 * \Delta Q3(0.05)) \end{pmatrix} \quad (29)$$

where k_2, k_3 – coefficients that take into account the average difference in tariffs;

They will take the values k_2 = 15, k_3 =250, L =3.

Recommendations for the practical application of the developed methodology.

The peculiarity of the operation and the distinction of the developed methodology will be the following:

1. Feature when creating profiles of objects:

- For each group of connecting lines and for each direction of the channel, describes the list of valid addresses of the source party, the list of uncontrolled addresses of the source party, lists of objects that have more than one address in the corresponding list of addresses.

- If a record of object profile information is not found during call processing, it must be generated automatically.

2. Specific profile formation:

If there is a loss in the System of call information for any period, to prevent failures in the formation of information about the profiles of objects, you must check all objects again, using zero values of traffic at the beginning of the period and restore information in profiles at the end.

For ease of use, the user interfaces and methods of working with them must be identical to the System as a whole. But in addition you need to consider the following:

1. The subsystem must contain means of actively informing users about events that need attention, by generating screen messages in the client part of the system, including at the start of the client part, if the event occurred and was not covered before.

2. Provide the ability to graphically display the characteristics of the profile of objects.

3. Provide for the possibility of organizing additional checks, with a slight change in the rules used in the analysis using the rule editor.

Areas of further research.

Further research should be aimed at improving the software for automated software, in order to enable automated recognition and operational implementation of traffic analysis for further detailed analysis of automated systems.

3. Conclusions

The analysis showed the absence of scientific and methodological apparatus, universal devices or automated software packages to ensure the rapid implementation of traffic analysis and information transfer to automated systems or relevant specialists. Therefore, a method has been developed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The developed method allows to carry out operative (real-time) informing of responsible specialists, or transfer of necessary data to the automated complex, about deviation of character of traffic from network elements (separate telephone numbers, number capacities, trunk groups, etc.) which is fixed in primary data. Deviations, the nature of traffic from the elements of network parameters are measured from the usual traffic of the telephone network relative to these elements.

The given technique takes into account practical recommendations concerning constant coefficients, calculations. These coefficients are selected by calculation and empirical. This reduces the response of the System using the developed method to the deviation of the communication parameters by 9% compared to existing methods. This is a perfectly acceptable result.

4. References

[1] Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp 8725-8729

[2] Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)

Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

[3] Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

[4] Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31.

[5] Milov O., Yevseiev S. Milevskyi S. Ivanchenko Y., Nesterov O., Puchkov O., Yarovyi A., Salii A., , Tiurin V., Timochko O. Development the model of the antagonistic agent's behavior under a cyber-conflict. Eastern European Journal of Advanced Technologies. Kharkiv. 2019. 4/9 (100). pp. 6–19

[6] S. Korotin, Y. Kravchenko, O. Starkova, K. Herasymenko, R. Mykolaichuk, "Analytical determination of the parameters of the self-tuning circuit of the traffic control system on the limit of vibrational stability", International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T`2019 – Proceedings, pp. 471–476.

[7] Y. Kravchenko, O. Leshchenko, N. Dakhno, O. Trush, O. Makhovych "Evaluating the effectiveness of cloud services", IEEE International Conference on Advanced Trends in Information Theory, ATIT`2019 – Proceedings, pp.120–124.

[8] A.M.Samoilenko, V.G.Samoilenko, V.V.Sobchuk. On periodic solutions of the equation of a nonlinear oscillator with pulse influence Ukrainian Mathematical Journal, 1999 (51), 6 Springer New York – P. 926-933

[9] V. Sobchuk et al .Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. Statistics Opt. Inform. Comput., Vol. 6, June 2018, pp 233–239.

[10] O. Barabash, N. Dakhno, H. Shevchenko, V. Sobchuk. Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method. IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) – Ukraine, Kyiv, 16 October 2018. pp. 94 – 97.

[11] S. Toliupa, N. Lukova-Chuiko, O. Oksiuk. Choice of Reasonable Variant of Signal and Code Constructions for Multirays Radio Channels. Second International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. IEEE PIC S&T 2015. pp. 269 – 271.

[12] N.Lukova-Chuiko, I. Ruban, V. Martovytskyi Designing a monitoring model for cluster supercomputers. Eastern-European Journal of Enterprise Technologies.- № 6(2) . 2016. P.32-37.

[13] N. Lukova-Chuiko, I. Ruban, V. Martovytskyi. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System.Cybernetics and Systems AnalysisV. 54. № 2. pp. 142 – 150. 2018.

[14] N.Lukova-Chuiko, I. Ruban, H. Khudov, O. Makoveichuk, I. Khizhnyak. Method For Determining Elements of Urban Infrastructure Objects Based On The Results From Air Monitoring.Eastern-European Journal of Enterprise Technologies. – № 4/9 (100). – 2019. – P. 52 – 61.

[15] N. Lukova-Chuiko, I Ruban, V. Martovytskyi, A. Kovalenko. Identification in Informative Systems on the Basis of Users' Behaviour. 2019 IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL), Sozopol. Bulgaria. pp. 574-577. 2019.

[16] N. Lukova-Chuiko, V. Saiko, V. Nakonechnyi, T. Narytnyk, M. Brailovskyi. Terahertz Range Interconnecting Line For LEO-System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, pp. 425-429. 2020.

[17] Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.