ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

ХАБАРШЫСЫ

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

PUBLISHED SINCE 1944

6

NOVEMBER – DECEMBER 2019

ALMATY, NAS RK

Clarivate Analytics

NAS RK is pleased to announce that Bulletin of NAS RK scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
http://www.bulletin-science.kz/index.php/en/

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 6, Number 382 (2019), 6 – 23 **https://doi.org/10.32014/2019.2518-1467.141**

UDC 621.39:004.05
IRSTI 81.93.29

Nazym Zhumangaliyeva[1], Aliya Doszhanova[2], Anna Korchenko[3]

[1]Kazakh National Research Technical University after K. I. Satpayev, Almaty, Kazakhstan,
[2]Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan,
[3]Department of Information Technology Security, National Aviation University, Kyiv, Ukraine.
E-mail: nazym_k.81@mail.ru, d_alia.81@mail.ru, annakor@ukr.net

ALGORITHMIC AND SOFTWARE SUPPORT FOR THE FORMATION OF PARAMETER STANDARDS FOR THE CYBER ATTACKS DETECTION SYSTEMS

Abstract. The vast majority of intrusion detection systems are becoming an integral part of the protection of any network security, they are used to monitor suspicious activity in the system and to detect the attacking actions of unauthorized side. Activation of cyber attacks initiates the creation of special technical solutions that can remain effective when new or modified types of cyber threats appear with unidentified or indistinctly defined properties. Most of these systems are aimed at identifying suspicious activity or interfering to the network in order to take adequate measures to prevent cyber attacks. Actual intrusion detection systems are those that are focused on identifying anomalous states but they have several disadvantages. More effective are expert approaches based on the use of knowledge and experience of specialists of the relevant subject area. Creation of technical solutions and special tools (for example, software for attack detection systems, which allow to detect previously unknown cyber attacks by monitoring the current state of indistinct parameters in a weakly formalized environment), based on expert approaches, is a promising area of research. Based on the well-known cyber attack detection system, which is based on an anomaly detection methodology (generated by cyber attacks) and a variety of relevant methods and models of the proposed software, which, due to the basic algorithm and a set of developed procedures (coordinate grid configuration; initialization of values based on a set of databases data and modules; graphical formation of parameters; search for common points according to the basic rules and graphical interpretation of the result) allow to automate the parameter standards formation process for modern intrusion detection systems and to reflect the results of the detection of anomalous state in a predetermined time interval.

Keywords: attacks; cyber attacks; anomalies; intrusion detection systems; attack detection systems; cyber attack detection systems; detection of anomalies in information systems.

1. Algorithmic and software support for cyber attack detection systems. According to the proposed structural solution of CPS which is based on CSFM, which is based on CMAS and the methods of ESFM and DEFM we construct and conduct an experimental research of algorithmic and software support for the formation of parameters standards for anomalies detection systems. [1, 2]), Such software operates on the basis of the basic algorithm System_level_Click algorithm (figure 1.1), combining a set of the following predefined processes (procedures):

* Coordinate_axes (construction of a coordinate grid);

* Convert_List (initialization of values based on CDB and EDB and IVFM. According to the structure of CPS, there are determined coordinates of standart and current LF in mi-measured parametric subtool figure 1.1) [3, 4];

* Graph_Build (graphical formation of parameters, for example, = = and = = and their reflections on the Canvas object according to step 3 [1];

* Crossing (IntersectionPoint and GetPoint procedures implementation and the reflection of the current state of the system in accordance with the basic rules in the detection environment)

* Rect_Area (two-dimensional support areas are created in accordance with the specified rules that come from the PDB which are formed on the basis of parametric sub-tools and are used to identify cyber attacks of various dimensions) [20, 21]);

* Line_point_Area reflects the common points of the design lines of the standard and current LF, for example, for parameters = = and = in a 2-dimensional parametric sub-environment.

Let consider the principle of operation of the main algorithm System_level_Click (figure 1.3), which integrates the specified procedures in order to create a complete list of graphical components necessary for the effective detection of an anomalous state in information systems [20].

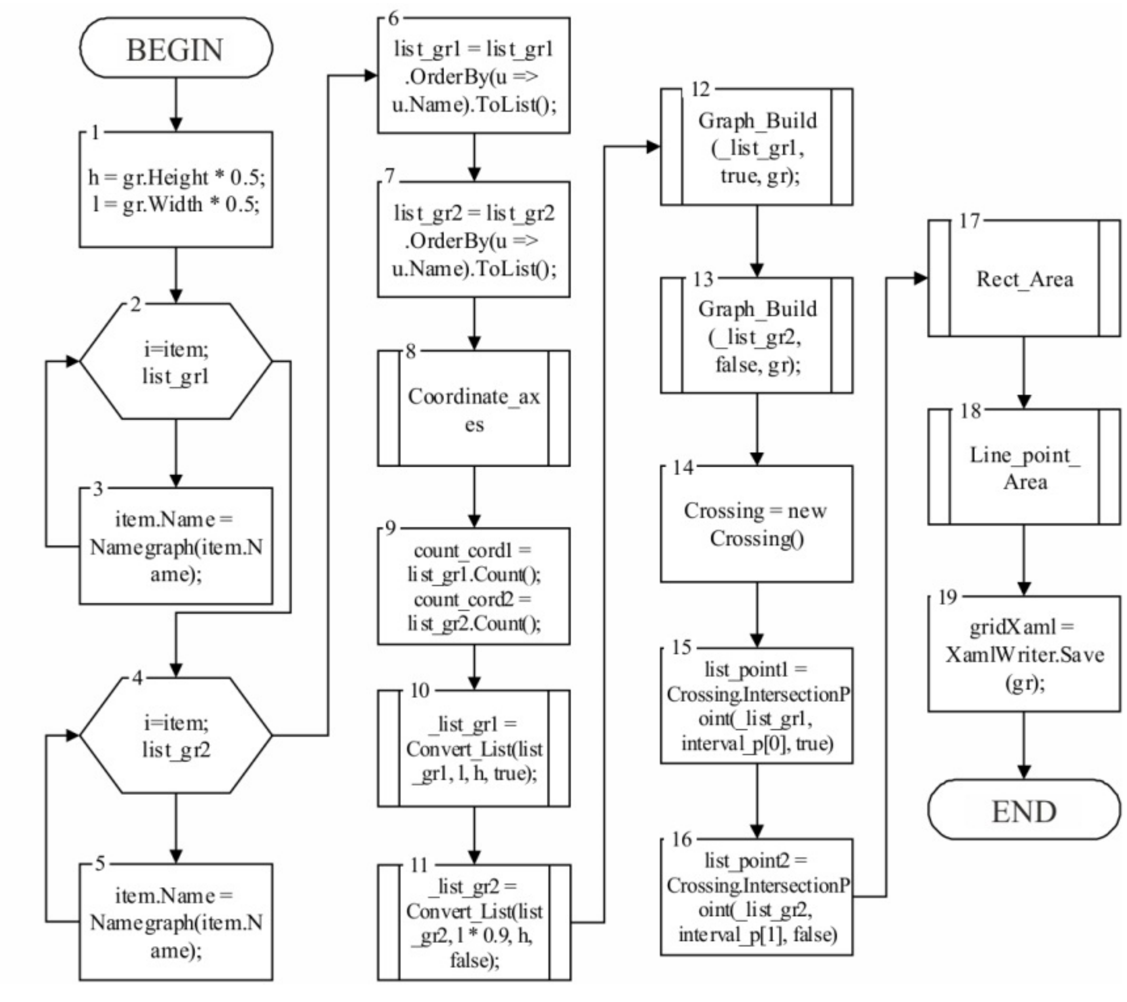


Figure 1.1 – Basic algorithm System_level_Click

At the beginning of the computational process (figure 1.3, vertex 1) there are initialized the necessary console characteristics.

Further (figure 1.3, vertex 2-3 and 4-5), respectively, we obtain in the cycles the initial data from the EDB [31], for example, for the NSC and NPSA parameters. Next (figure 1.2, vertex 6-7) there are formed sets of order of parameter matching. Next (figure 1.3, vertex 8) there is implemented a predefined process (class Coordinate_axes), according to which the procedure Main_coordinate_axes is executed (figure 1.4), performing sequential processing of three graduation programs [10, 14]:

* Grid_coordinates (responsible for the creation of a scalable coordinate grid);

* Graduation_axes (responsible for marking axes and graduation intervals in the scalable area);

* Drawing_axes (responsible for the creation of axes to display the required parameters, for example, = = and = = in 2-dimensional parametric environment (Further, according to the structure of CPS there is determined the amount of data (count_cord1 and count_cord2) in EDB for each of the parameters, for example, = = and =

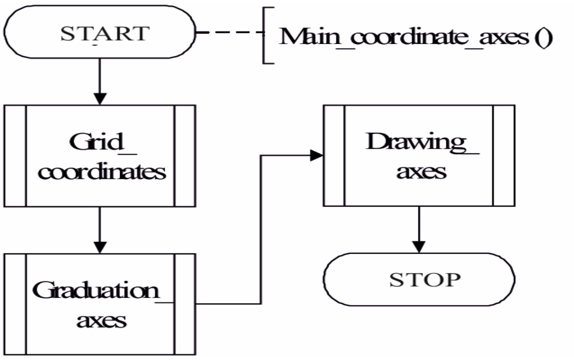


Figure 1.2 – Algorithm Main_coordinate_axes

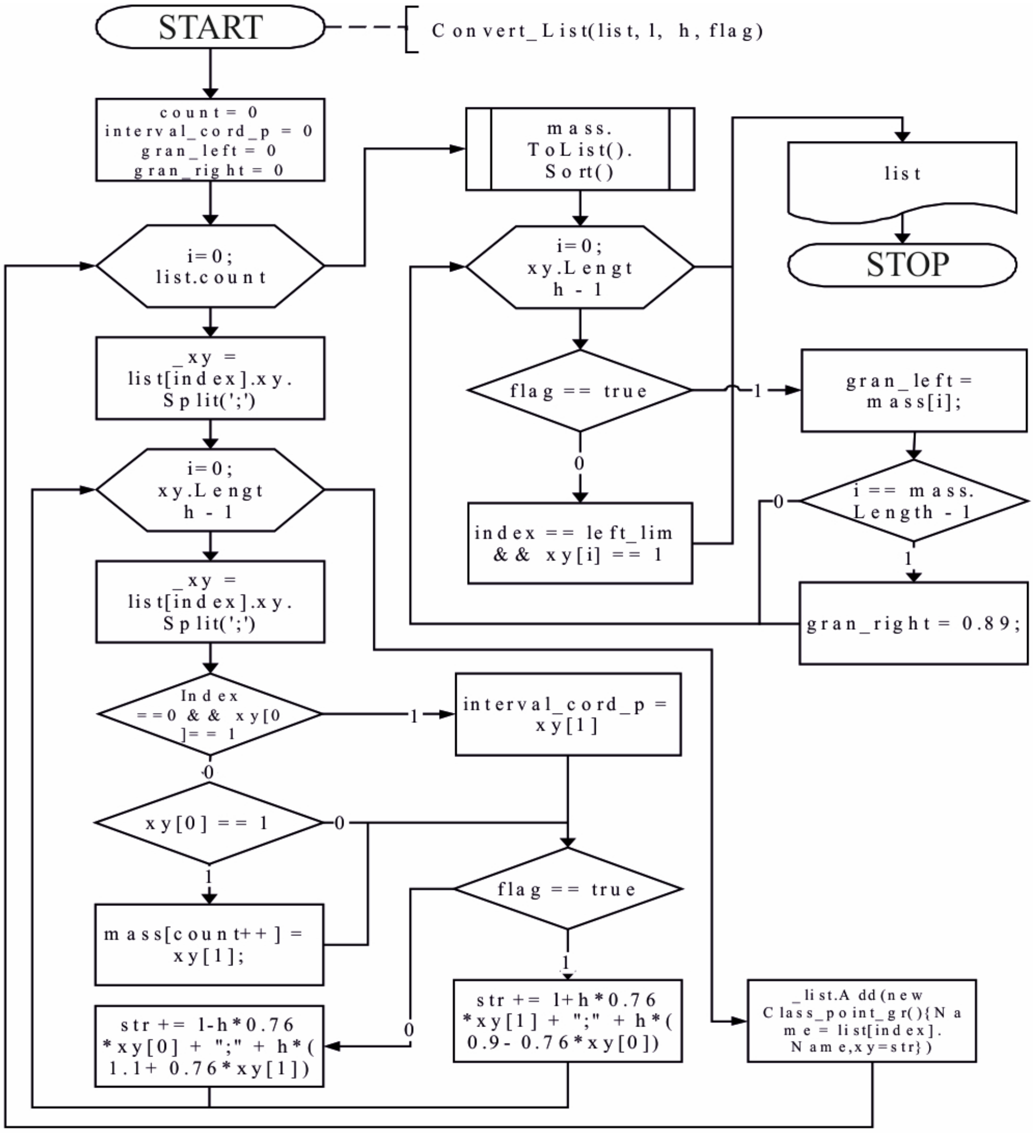


Figure 1.3 – Algorithm of Convert_List implementation

At the next stage (vertices 10 and 11) there is called the procedure Convert_List which allows to receive data from the tables with specified parameters according to, for example, NSC and NPSA, which are converted into the necessary form in order to create graphical images of the specified parameters, for example, = = and = = in a 2-dimensional parametric environment.

The process of converting data consists of two stages. The first, according to the step 4, determines the interval to which the vertex of the graphical image of the current LF belongs in mi-dimensional parametric environment .

This is necessary for the search for common points of graphical images of the standard and current LF, since these points must lie within the same limits with the vertex of any of the parameters.

The second one converts standard and current LF, which are in the EDB and IVFM, into values corresponding to the Canvas coordinate system. This procedure returns a list of convertible LF values and boundaries, which can contain common points of the graphical image of the current state, for example, for the parameters.

The obtained data are necessary for the construction of projections and common points of graphical images according to the specified parameters of NSC and NPSA.

Further (figure 1.4, vertices 12-13) there is called the Graph_Build procedure (figure 1.5, 1.6), on the basis of the EDB and IVFM, it allows to create graphical images of the standard and current LF.

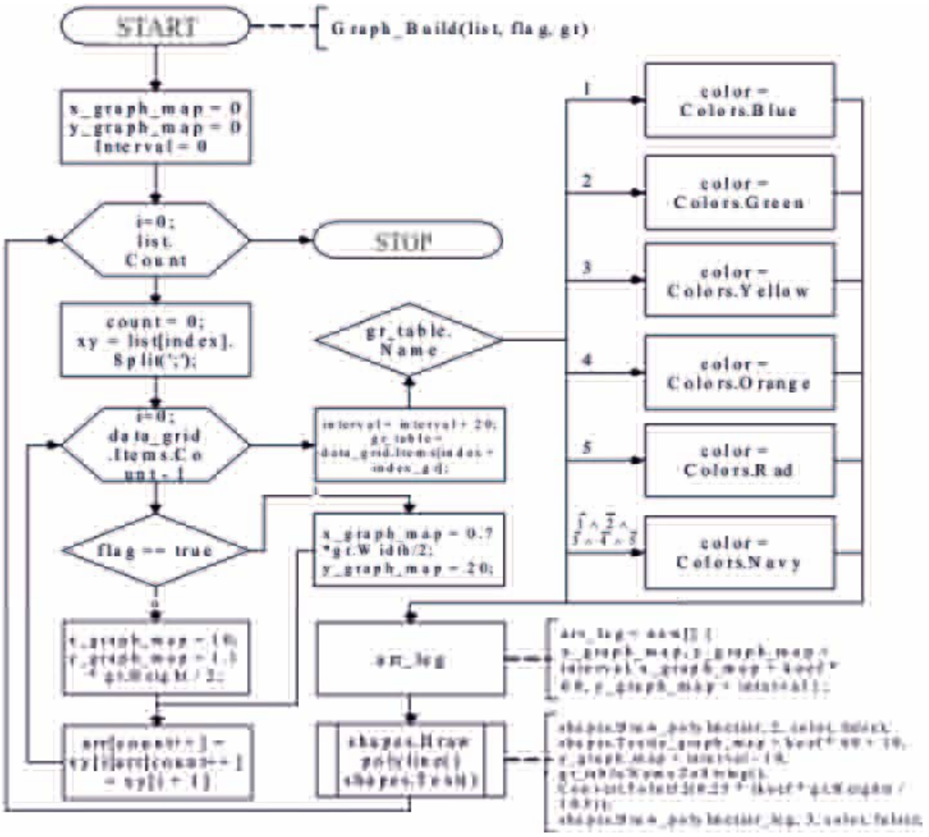


Figure 1.4 – Algorithm of Graph_Build implementation

After the process of data converting from EDB, they are transferred to the Graph_Build program, which, recieves the list of converted data as an index to get the color and to change the Canvas graphical object for the basic values creation. Using the Main_figures there is created the object of the *shapes* class in the Graph_Build and then using the figures Draw_polyline is called and the data from the list is written to the array. Variations of colors and types of lines are also determined. Performing in the cycle of the specified sequence of actions is associated with the construction of graphical images and their legends (for example, "P", "OM", "M", "S", "B" and "V" for the parameters = = and = = (see figure 1.6) in a two-dimensional parametric environment.

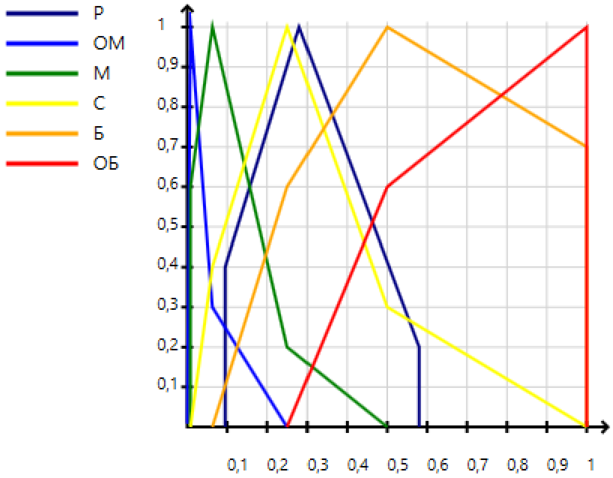


Figure 1.5 – The result of the procedure Graph_Build for the NSC parameter

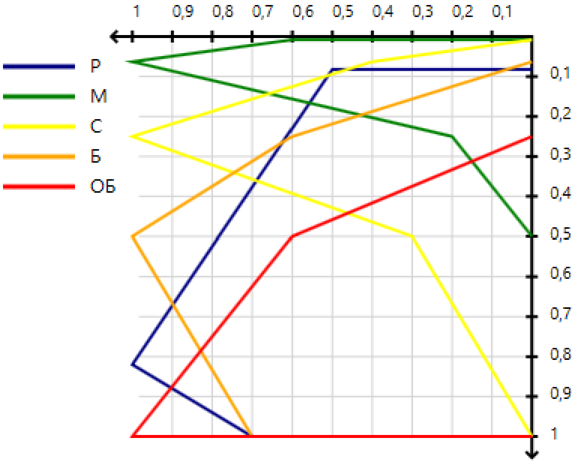


Figure 1.6 – The result of the procedure Graph_Build for the NPSA parameter

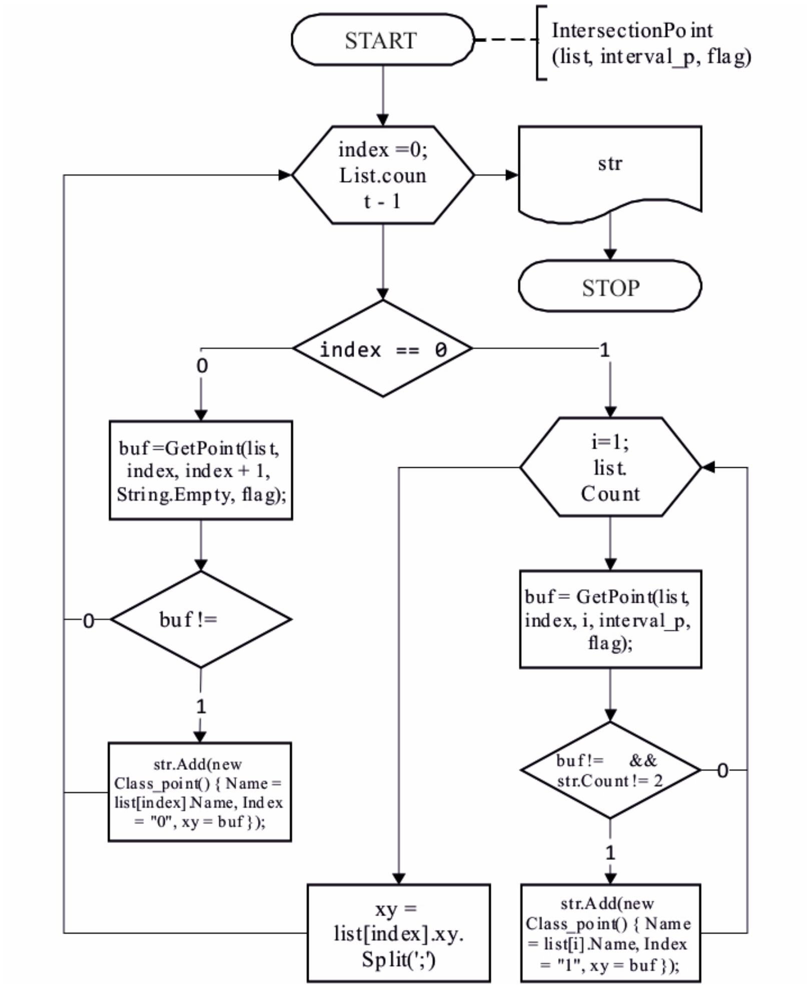


Figure 1.7 – Algorithm of IntersectionPoint procedure implementation

At the next stage (figure 1.1, vertex 14) there is created an object of the *Crossing* class and the Intersection Point procedure is called and is formed a list of coordinates of common points necessary to reflect the current state of the system.

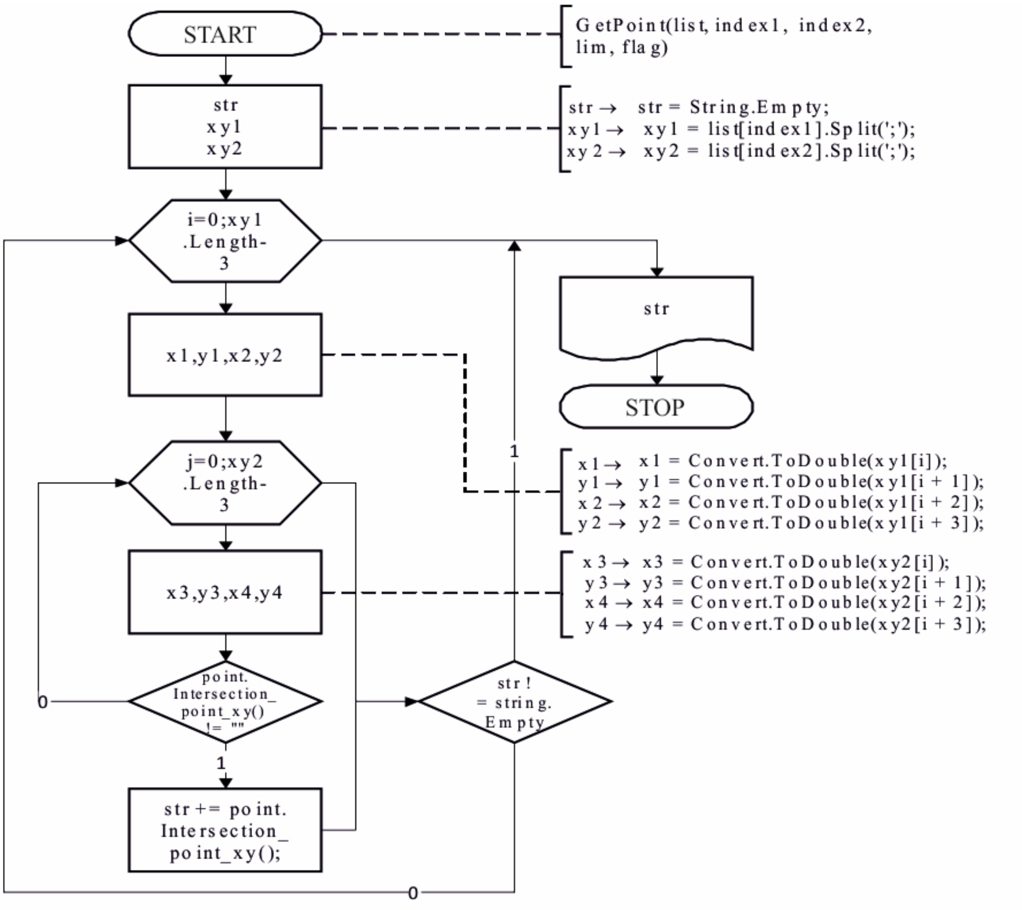

START
GetPoint(list, index1, index2, lim, flag)
str
xy1
xy2
str → str = String.Empty;
xy1 → xy1 = list[index1].Split(';');
xy2 → xy2 = list[index2].Split(';');
i=0;xy1 .Length-3
str
STOP
x1,y1,x2,y2
1
x1 → x1 = Convert.ToDouble(xy1[i]);
y1 → y1 = Convert.ToDouble(xy1[i + 1]);
x2 → x2 = Convert.ToDouble(xy1[i + 2]);
y2 → y2 = Convert.ToDouble(xy1[i + 3]);
j=0;xy2 .Length-3
x3,y3,x4,y4
x3 → x3 = Convert.ToDouble(xy2[i]);
y3 → y3 = Convert.ToDouble(xy2[i + 1]);
x4 → x4 = Convert.ToDouble(xy2[i + 2]);
y4 → y4 = Convert.ToDouble(xy2[i + 3]);
0
point. Intersection_ point_xy() != ""
str ! = string. Empty
1
str += point. Intersection_ point_xy();
0

Figure 1.8 –Algorithm of get point procedure implementation

Obtained list and identifiers of standard LF with the help of Convert_List (figure 1.1, vertices 10-11) there are determined the parameters of identification of standard areas with the help of Draw_main_rect. [8, 9].

It should be noted that the *Crossing* class consists of two procedures:

• IntersectionPoint (figure 1.9);

• GetPoint (figure 1.10).

The first *Intersection Point* procedure allows to obtain common points of graphical images (separately for each of the parameters), as well as with adjacent standard LF (see step 5 and 6). At the next stage (figure 1.3, vertex 14) there is created an object of the *Crossing* class and the *Intersection Point* procedure is called and is formed a list of coordinates of common points necessary to reflect the current state of the system. Obtained the list and identifiers of standard LF with the help of Convert_List (figure 1.1, vertices 10-11) there are determined the parameters of identification of support areas with the help of Draw_main_rect. It should be noted that the *Crossing* class consists of two procedures:

• IntersectionPoint (figure 1.7);

• GetPoint (figure 1.8).

The first *Intersection Point* procedure allows to obtain common points of graphical images (separately for each of the parameters), as well as with adjacent standard LF.

The second GetPoint procedure is responsible for obtaining the coordinates of the above-mentioned points, that is, for example, a pair of values that characterize the component of the first graphical image and a pair of values of the second one. Further, all possible values for the selected component of the first graphical image are calculated relative to all possible components of the second one. The calculation is performed using Intersection_point, which defines the common points of the component for the given coordinates and returns to Get Point.

Next (figure 1.1, vertices 15-16) there is implemented the intersection_point class (in accordance with the functions of MARN and MDIT - see the CPS structure consisting of two Intersection_point procedures (figure 1.9) and Intersection_point_xy (figure 1.11).

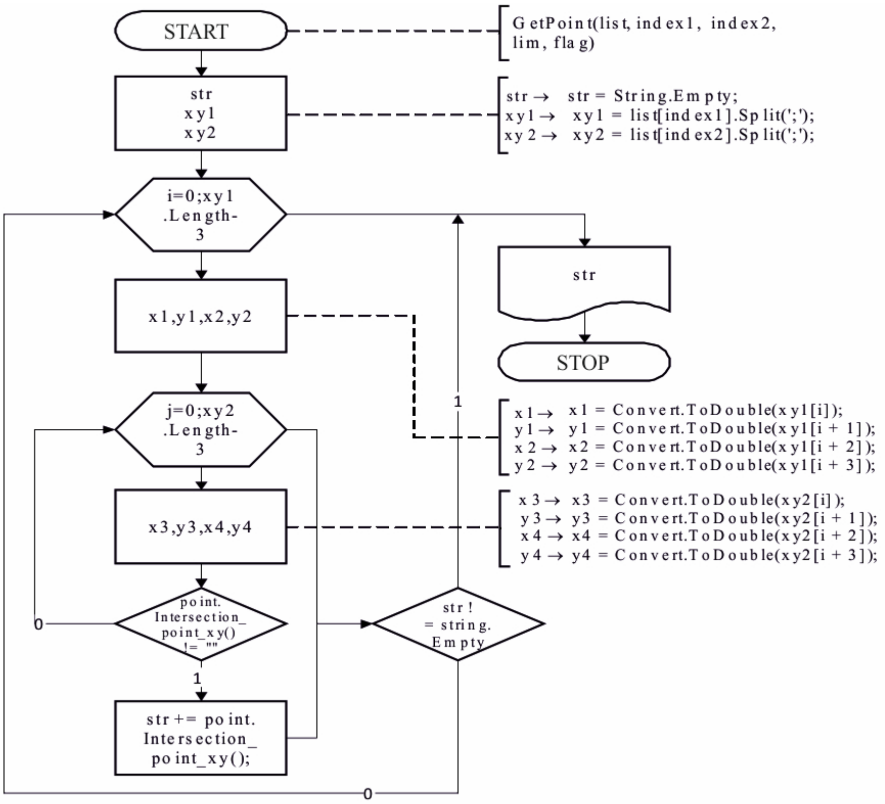

START
GetPoint(list, index1, index2, lim, flag)
str
xy1
xy2
str → str = String.Empty;
xy1 → xy1 = list[index1].Split(';');
xy2 → xy2 = list[index2].Split(';');
i=0;xy1.Length-3
str
STOP
x1,y1,x2,y2
1
x1 → x1 = Convert.ToDouble(xy1[i]);
y1 → y1 = Convert.ToDouble(xy1[i + 1]);
x2 → x2 = Convert.ToDouble(xy1[i + 2]);
y2 → y2 = Convert.ToDouble(xy1[i + 3]);
j=0;xy2.Length-3
x3,y3,x4,y4
x3 → x3 = Convert.ToDouble(xy2[i]);
y3 → y3 = Convert.ToDouble(xy2[i + 1]);
x4 → x4 = Convert.ToDouble(xy2[i + 2]);
y4 → y4 = Convert.ToDouble(xy2[i + 3]);
0
point.Intersection_point_xy() != ""
str != string.Empty
1
str += point.Intersection_point_xy();
0

Figure 1.9 – Algorithm of Intersection_point procedure implementation

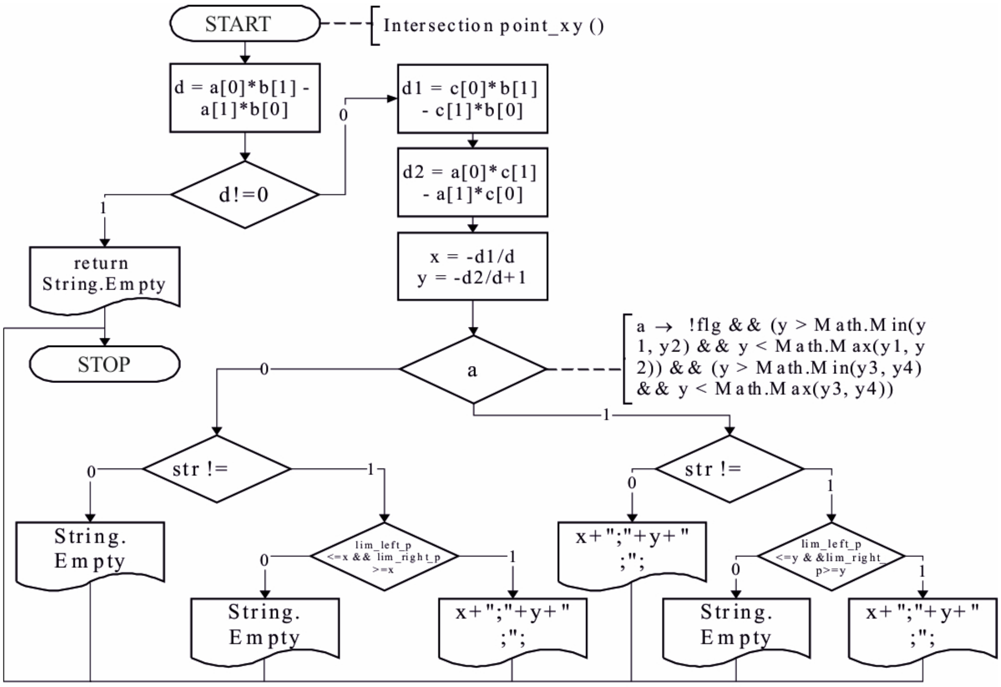

START
Intersection point_xy ()
d = a[0]*b[1] - a[1]*b[0]
0
d1 = c[0]*b[1] - c[1]*b[0]
d!=0
1
d2 = a[0]*c[1] - a[1]*c[0]
return String.Empty
x = -d1/d
y = -d2/d+1
STOP
a → !flg && (y > Math.Min(y1, y2) && y < Math.Max(y1, y2)) && (y > Math.Min(y3, y4) && y < Math.Max(y3, y4))
0
a
1
0
str !=
1
0
str !=
1
String.Empty
lim_left_p <=x && lim_right_p >=x
0
1
x+";"+y+";";
lim_left_p <=y & &lim_right_p>=y
0
1
String.Empty
x+";"+y+";";
String.Empty
x+";"+y+";";

Figure 1.10 – Algorithm of Intersection_point_xy procedure implementation

In turn, the first one is a constructor that receives data from GetPoint (figure 1.9) and determines the coefficients that are transmitted to the second –Intersection_point_xy, where common points are calculated and returned to GetPoint [4, 6].

At the next stage (figure 1.1, vertex 17) there is called the Rect_Area procedure (in accordance with the functions of PDB and MRA, see the CPS structure (figure 1.12), which is responsible for constructing basic two-dimensional areas and current state areas, and sequentially activates Draw_main_rect (figure 1.13) and Draw_Rect. The procedure Draw_main_rect is responsible for the construction of two-dimensional standard areas, taking into account the rules on the basis of which the level of the anomalous state of the system will be determined.

Depending on the obtained data on visualization, for example, parameters = = = and on the basis of common points of graphical images of standard LF and projections of linear components constructed using the class Draw_main_ object, we obtain the necessary standard areas. They are generated according to the above defined rules, therefore, the graphical image generates colored areas that reflect the level of the anomalous state of the system in the detection environment.

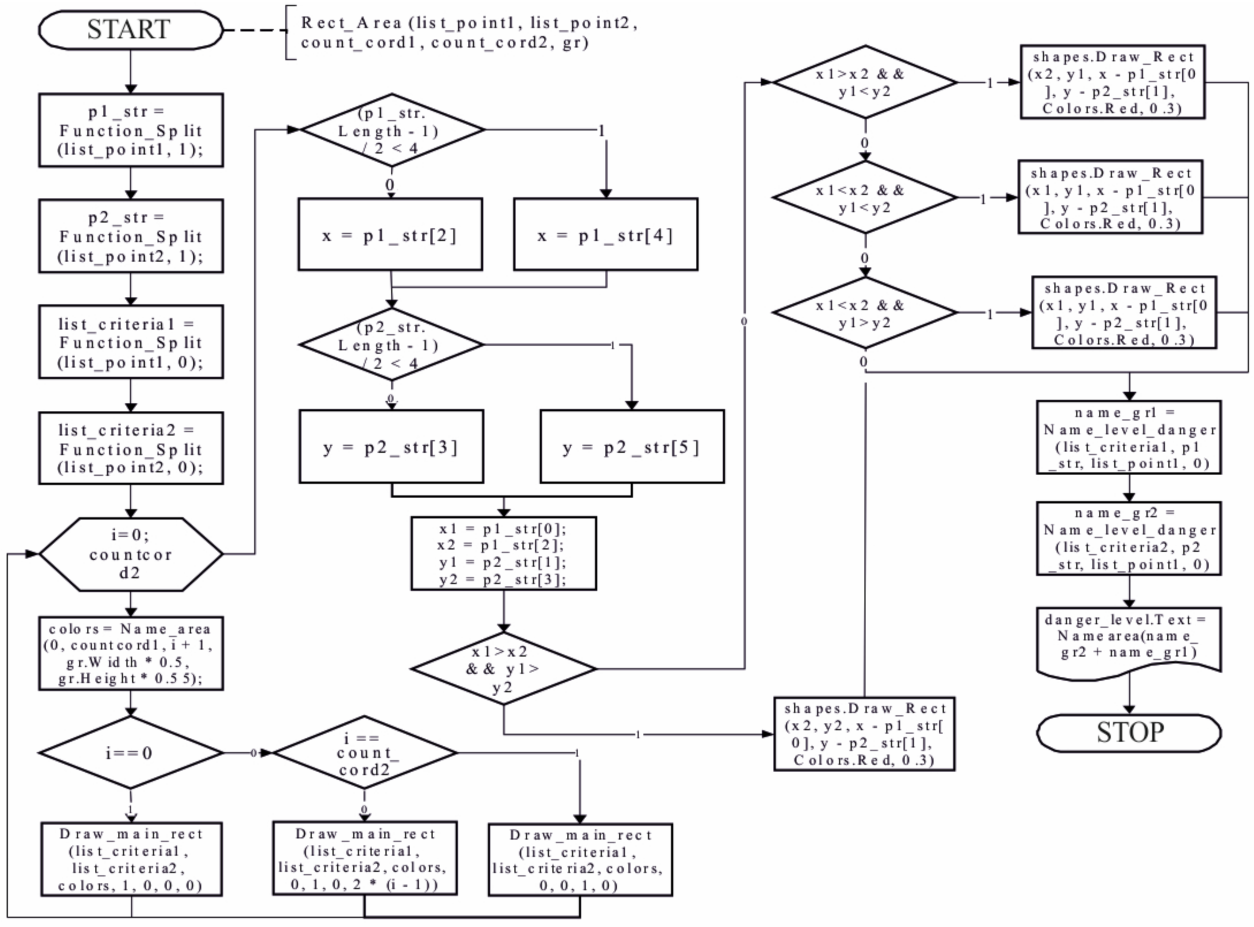
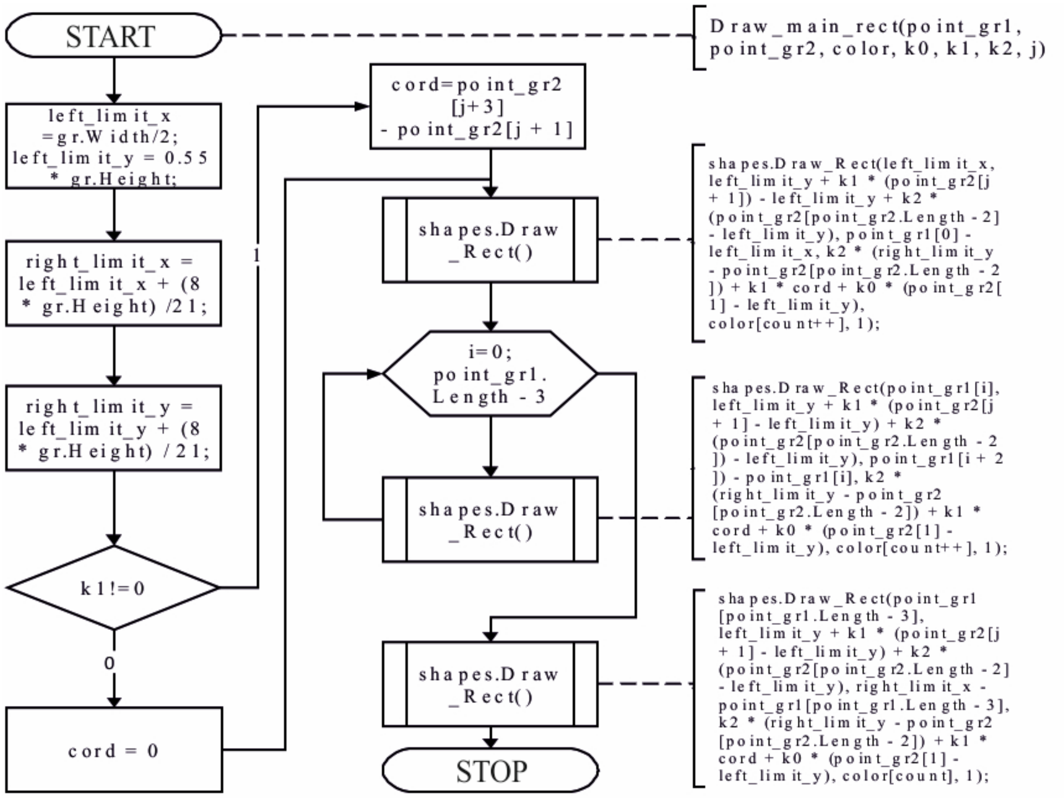

START
Rect_Area (list_point1, list_point2, count_cord1, count_cord2, gr)
p1_str = Function_Split (list_point1, 1);
p2_str = Function_Split (list_point2, 1);
list_criteria1 = Function_Split (list_point1, 0);
list_criteria2 = Function_Split (list_point2, 0);
i=0; countcord2
colors= Name_area (0, countcord1, i + 1, gr.Width * 0.5, gr.Height * 0.55);
i==0
1
0
i == count_cord2
Draw_main_rect (list_criterial, list_criteria2, colors, 1, 0, 0, 0)
Draw_main_rect (list_criterial, list_criteria2, colors, 0, 1, 0, 2 * (i - 1))
Draw_main_rect (list_criterial, list_criteria2, colors, 0, 0, 1, 0)
(p1_str.Length - 1) / 2 < 4
x = p1_str[2]
x = p1_str[4]
(p2_str.Length - 1) / 2 < 4
y = p2_str[3]
y = p2_str[5]
x1 = p1_str[0];
x2 = p1_str[2];
y1 = p2_str[1];
y2 = p2_str[3];
x1>x2 && y1>y2
x1>x2 && y1<y2
x1<x2 && y1<y2
x1<x2 && y1>y2
shapes.Draw_Rect (x2, y1, x - p1_str[0], y - p2_str[1], Colors.Red, 0.3)
shapes.Draw_Rect (x1, y1, x - p1_str[0], y - p2_str[1], Colors.Red, 0.3)
shapes.Draw_Rect (x1, y1, x - p1_str[0], y - p2_str[1], Colors.Red, 0.3)
shapes.Draw_Rect (x2, y2, x - p1_str[0], y - p2_str[1], Colors.Red, 0.3)
name_gr1 = Name_level_danger (list_criterial, p1_str, list_point1, 0)
name_gr2 = Name_level_danger (list_criteria2, p2_str, list_point1, 0)
danger_level.Text = Namearea(name_gr2 + name_gr1)
STOP

Figure 1.11 – Algorithm of Rect_Area procedure implementation

Next (figure 1.1, vertex 18) there is called the Line_point_Area subprogram (in accordance with the MB - see the structure of SPK 1 (figure 1.14) and on the Canvas graphical object using the Draw_main_object class, calling its procedures: Draw_main_point (figure 1.15); Draw_main_line (figure 1.16) - there are created projections of linear components and common points, both on the initial graphical images and on the final image of the current state.


START
Draw_main_rect(point_gr1, point_gr2, color, k0, k1, k2, j)
left_limit_x =gr.Width/2; left_limit_y = 0.55 * gr.Height;
right_limit_x = left_limit_x + (8 * gr.Height) /21;
right_limit_y = left_limit_y + (8 * gr.Height) / 21;
k1!=0
1
0
cord = 0
cord=point_gr2 [j+3] - point_gr2[j + 1]
shapes.Draw_Rect()
shapes.Draw_Rect(left_limit_x, left_limit_y + k1 * (point_gr2[j + 1]) - left_limit_y + k2 * (point_gr2[point_gr2.Length - 2] - left_limit_y), point_gr1[0] - left_limit_x, k2 * (right_limit_y - point_gr2[point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count++], 1);
i=0; point_gr1. Length - 3
shapes.Draw_Rect()
shapes.Draw_Rect(point_gr1[i], left_limit_y + k1 * (point_gr2[j + 1] - left_limit_y) + k2 * (point_gr2[point_gr2.Length - 2]) - left_limit_y), point_gr1[i + 2]) - point_gr1[i], k2 * (right_limit_y - point_gr2 [point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count++], 1);
shapes.Draw_Rect()
shapes.Draw_Rect(point_gr1 [point_gr1.Length - 3], left_limit_y + k1 * (point_gr2[j + 1] - left_limit_y) + k2 * (point_gr2[point_gr2.Length - 2] - left_limit_y), right_limit_x - point_gr1[point_gr1.Length - 3], k2 * (right_limit_y - point_gr2 [point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count], 1);
STOP

Figur 1.12 – Algorithm of draw_main_rect procedure implementation

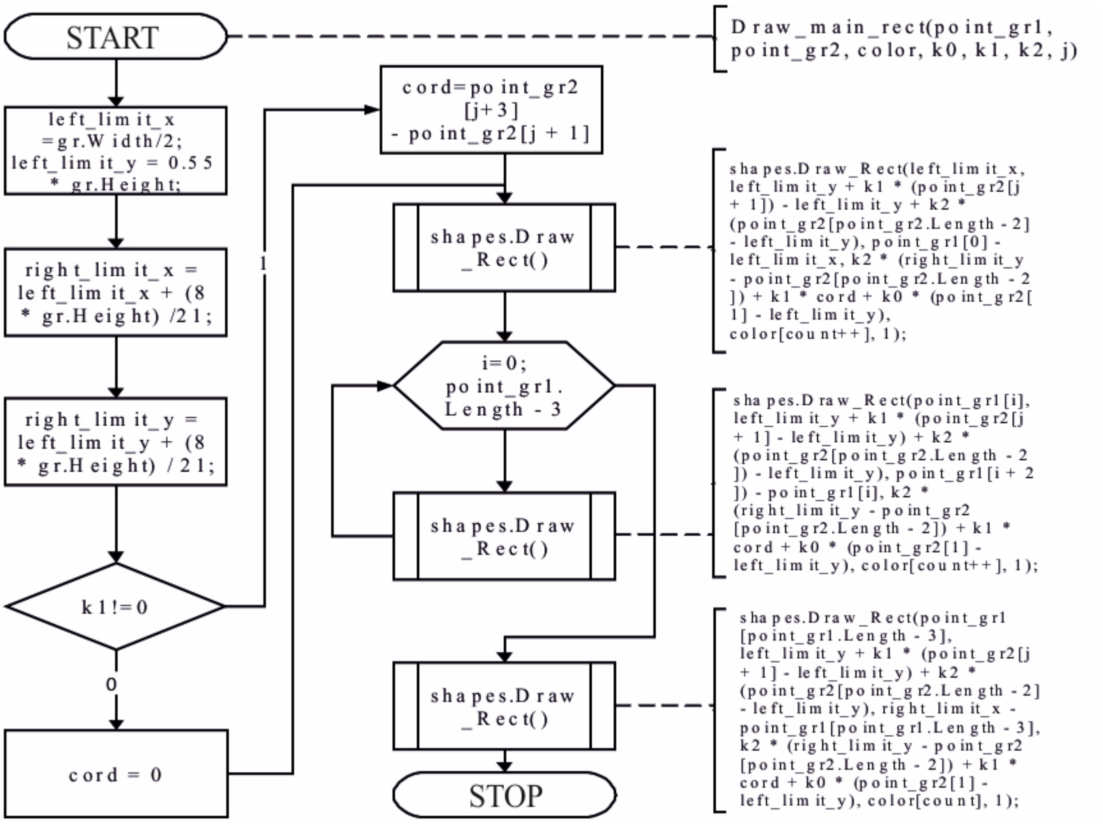

START
Draw_main_rect(point_gr1, point_gr2, color, k0, k1, k2, j)
left_limit_x =gr.Width/2; left_limit_y = 0.55 * gr.Height;
right_limit_x = left_limit_x + (8 * gr.Height) /21;
right_limit_y = left_limit_y + (8 * gr.Height) / 21;
k1!=0
1
0
cord = 0
cord=point_gr2 [j+3] - point_gr2[j + 1]
shapes.Draw_Rect()
shapes.Draw_Rect(left_limit_x, left_limit_y + k1 * (point_gr2[j + 1]) - left_limit_y + k2 * (point_gr2[point_gr2.Length - 2] - left_limit_y), point_gr1[0] - left_limit_x, k2 * (right_limit_y - point_gr2[point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count++], 1);
i=0; point_gr1. Length - 3
shapes.Draw_Rect()
shapes.Draw_Rect(point_gr1[i], left_limit_y + k1 * (point_gr2[j + 1] - left_limit_y) + k2 * (point_gr2[point_gr2.Length - 2]) - left_limit_y), point_gr1[i + 2]) - point_gr1[i], k2 * (right_limit_y - point_gr2 [point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count++], 1);
shapes.Draw_Rect()
shapes.Draw_Rect(point_gr1 [point_gr1.Length - 3], left_limit_y + k1 * (point_gr2[j + 1] - left_limit_y) + k2 * (point_gr2[point_gr2.Length - 2] - left_limit_y), right_limit_x - point_gr1[point_gr1.Length - 3], k2 * (right_limit_y - point_gr2 [point_gr2.Length - 2]) + k1 * cord + k0 * (point_gr2[1] - left_limit_y), color[count], 1);
STOP

Figure 1.13 – Algorithm of line_point_area procedure implementation

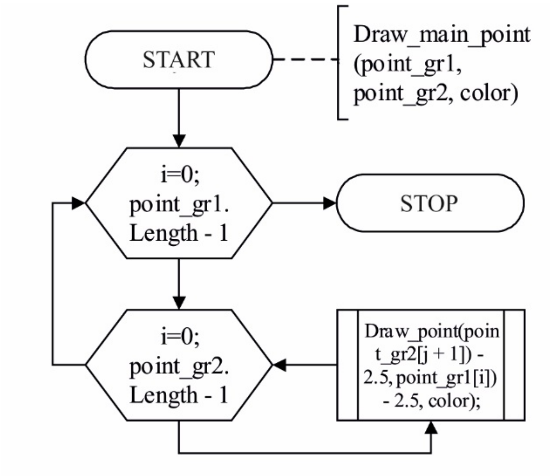


Figure 1.14 – Algorithm of Draw_main_point procedure implementation

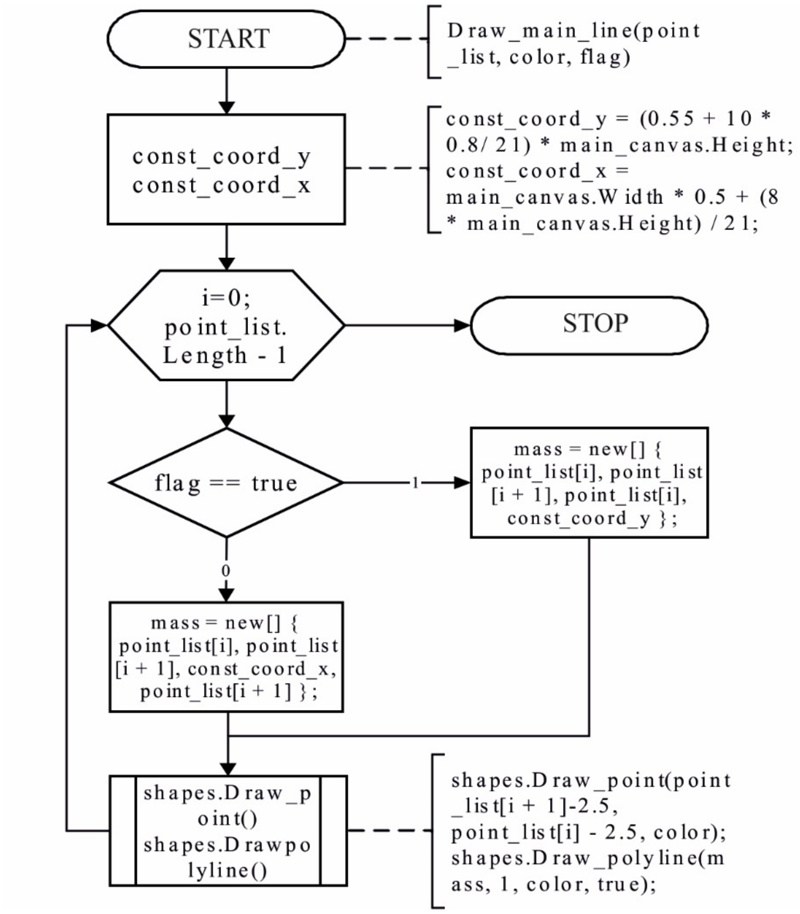


Figure 1.15 – Algorithm of Draw_main_point procedure implementation

Also, during the construction of graphical elements in the Sys-tem_level_Click algorithm (figure 1.3) there are are used additional components, for example, the Main_figures class includes procedures: Draw_polyline (figure 1.19); Draw_point; Draw_Rect (figure 1.20), which respectively form linear components with various input characteristics of points on the graphical object Canvasi. After all the data has been received, System_level_Click creates the current state area (according to the MB functionality — see the SEC structure), which allows to visually assess the anomalous position in the system to make the necessary decision.

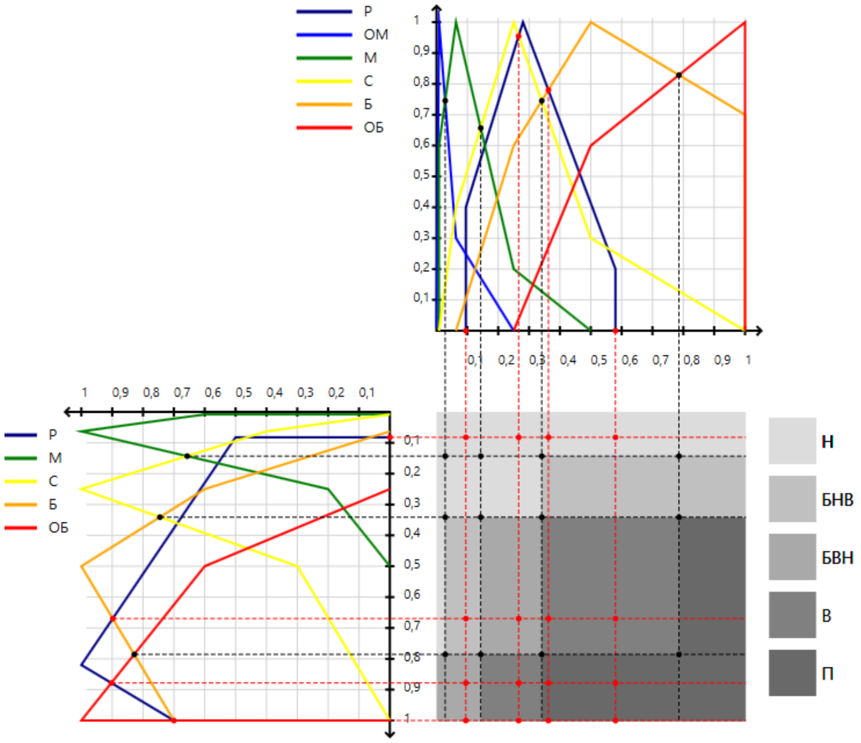


Figure 1.16 – An example of support areas creation in accordance with Draw_main_rect

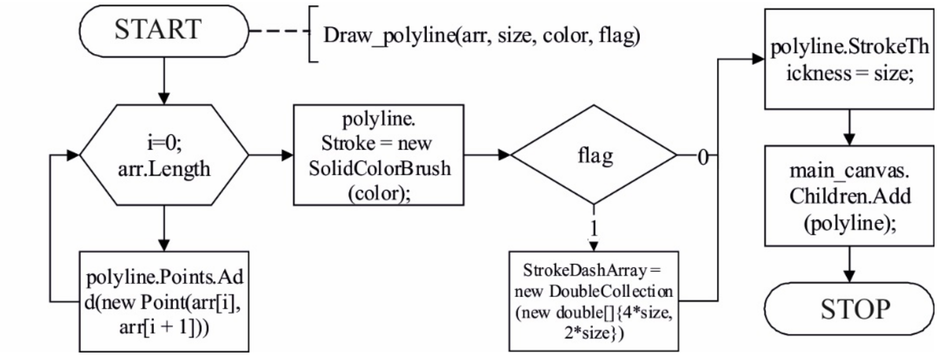

START
Draw_polyline(arr, size, color, flag)
i=0;
arr.Length
polyline.Points.Add(new Point(arr[i], arr[i + 1]))
polyline.
Stroke = new
SolidColorBrush
(color);
flag
0
1
StrokeDashArray = new DoubleCollection (new double[]{4*size, 2*size})
polyline.StrokeThickness = size;
main_canvas.
Children.Add
(polyline);
STOP

Figure 1.17 – Algorithm of Draw_polyline procedure implementation

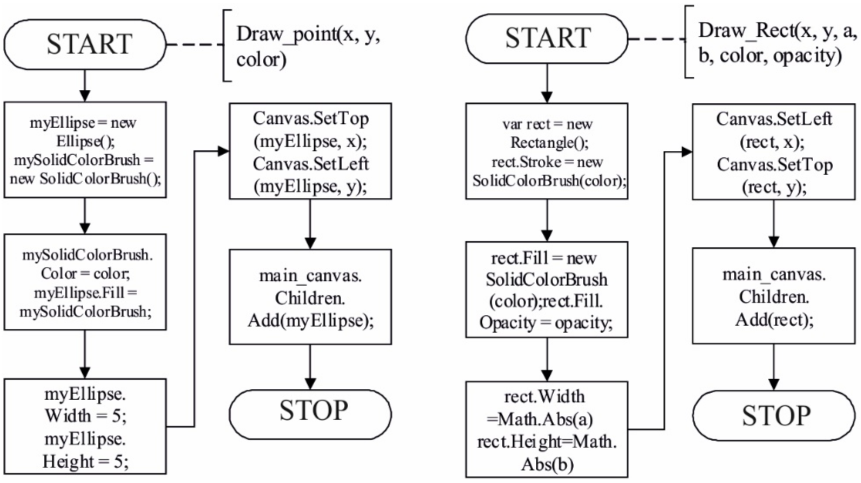
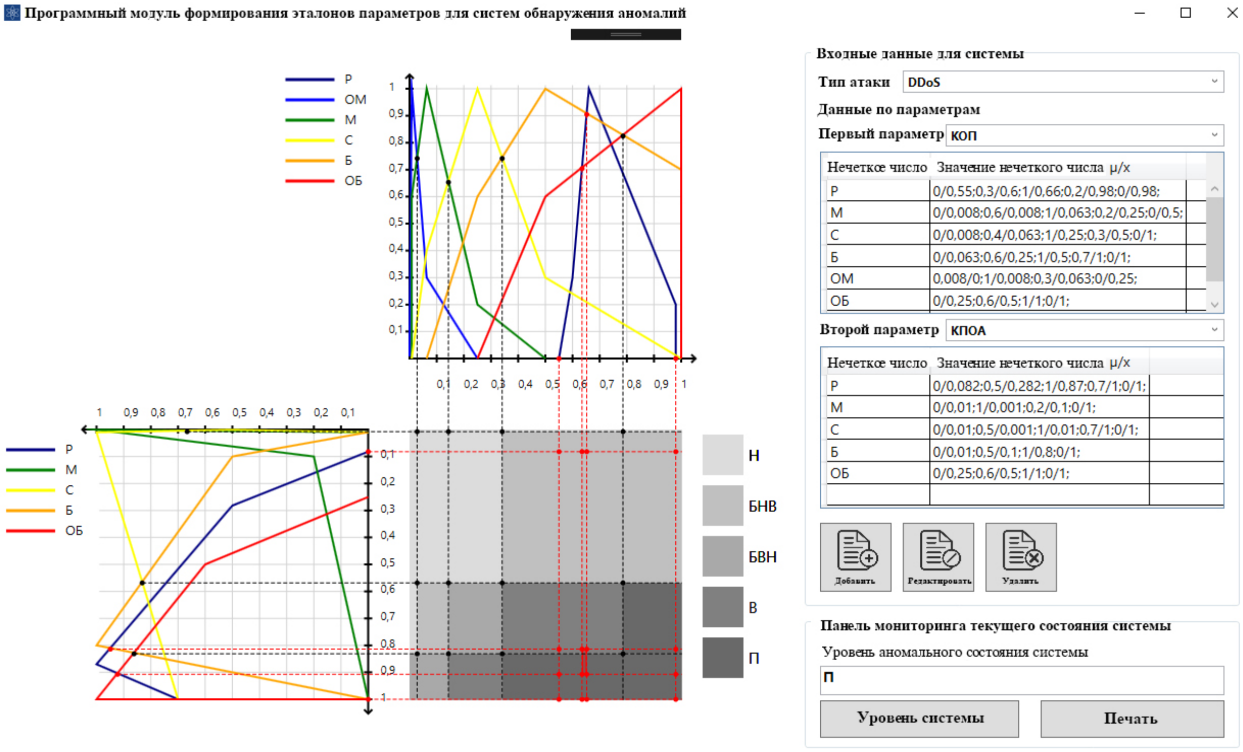


Figure 1.18 – Algorithm of draw_point and Draw_Rect procedures implementation



Программный модуль формирования эталонов параметров для систем обнаружения аномалий

Входные данные для системы

Тип атаки DDoS

Данные по параметрам

Первый параметр КОП

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,55;0,3/0,6;1/0,66;0,2/0,98;0/0,98;
М	0/0,008;0,6/0,008;1/0,063;0,2/0,25;0/0,5;
С	0/0,008;0,4/0,063;1/0,25;0,3/0,5;0/1;
Б	0/0,063;0,6/0,25;1/0,5;0,7/1;0/1;
ОМ	0,008/0;1/0,008;0,3/0,063;0/0,25;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

Второй параметр КПОА

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,082;0,5/0,282;1/0,87;0,7/1;0/1;
М	0/0,01;1/0,001;0,2/0,1;0/1;
С	0/0,01;0,5/0,001;1/0,01;0,7/1;0/1;
Б	0/0,01;0,5/0,1;1/0,8;0/1;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

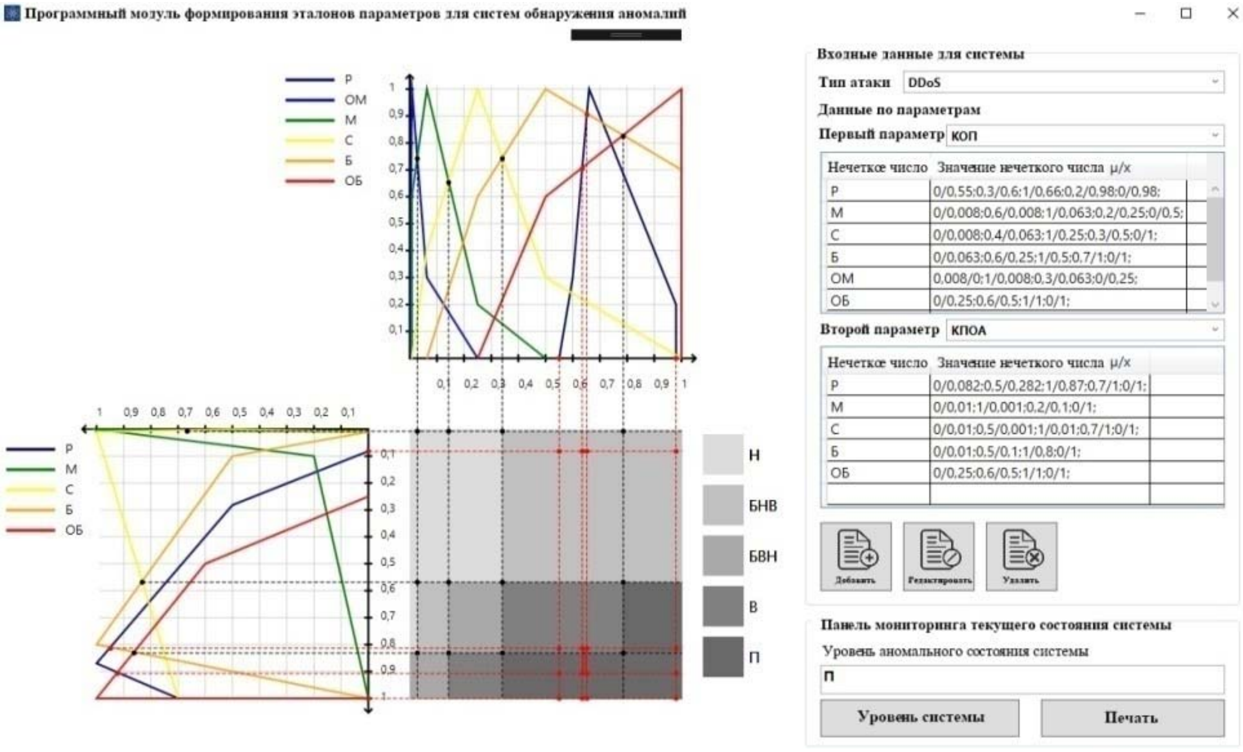
Панель мониторинга текущего состояния системы

Уровень аномального состояния системы

П

Figure 1.19 – An example of work on the formation of parameter standards (determination of the first current state of the system)

In fact, the procedure generates the current block, for example, in the form of a red rectangular area, which interprets the anomaly in a 2-dimensional parametric NSC-NPSA environment generated by the corresponding attacking SP-environment at the moment of time. An example of work on the formation of parameter standards with various experimental data is shown on figures 1.20 and 1.21.



Программный модуль формирования эталонов параметров для систем обнаружения аномалий

Входные данные для системы

Тип атаки DDoS

Данные по параметрам

Первый параметр КОП

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,55;0,3/0,6;1/0,66;0,2/0,98;0/0,98;
М	0/0,008;0,6/0,008;1/0,063;0,2/0,25;0/0,5;
С	0/0,008;0,4/0,063;1/0,25;0,3/0,5;0/1;
Б	0/0,063;0,6/0,25;1/0,5;0,7/1;0/1;
ОМ	0,008/0;1/0,008;0,3/0,063;0/0,25;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

Второй параметр КПОА

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,082;0,5/0,282;1/0,87;0,7/1;0/1;
М	0/0,01;1/0,001;0,2/0,1;0/1;
С	0/0,01;0,5/0,001;1/0,01;0,7/1;0/1;
Б	0/0,01;0,5/0,1;1/0,8;0/1;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

Панель мониторинга текущего состояния системы

Уровень аномального состояния системы

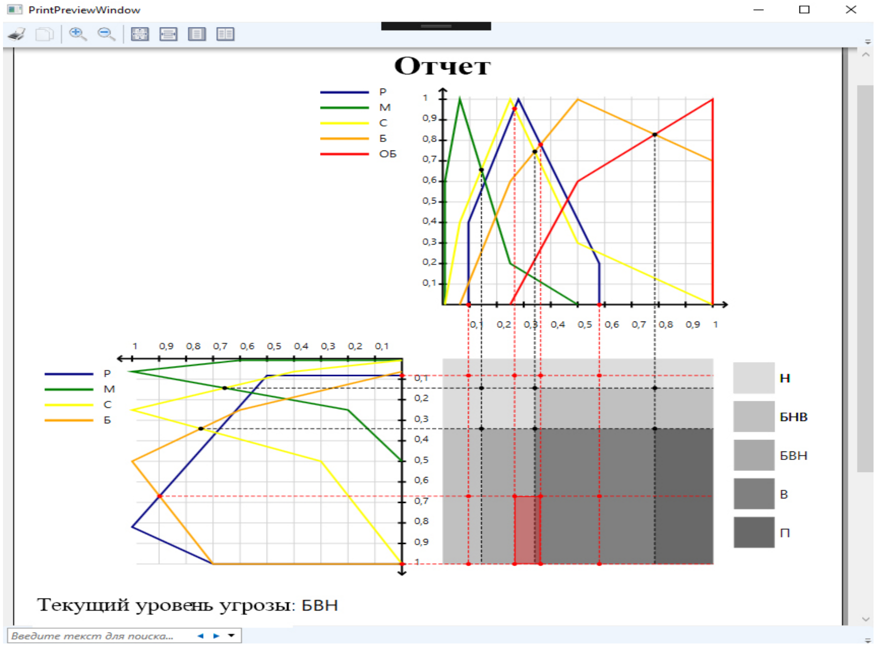
П

Figure 1.20 – Example of work on the formation of parameter standards (determination of the second current state of the system)

At the final stage (figure 1.2, vertex 19) there are used the *printpreviewwindow* and *Print* classes which are responsible for the creation of the report file and its preview. That is, the user, if necessary, at the time can initialize the print mode, which will create a preview file in the buffer memory (figure 1.22), which can be printed (figure 1.23) or saved in pdf format (figure 1.24).

Experimental research and practical use of the proposed basis of the developed algorithmic support. Printing is initiated as a "system level", as a result of which the canvas graphical object is converted into the XAML file, the rest of the text, the report title and the rule (according to the functionality, see the structure of the SPC) generated using the standard FixedDocument class, which allows convenient to place the text in the report.

The report file is transferred to the buffer memory, after which it can be viewed, changed print settings, and the like.

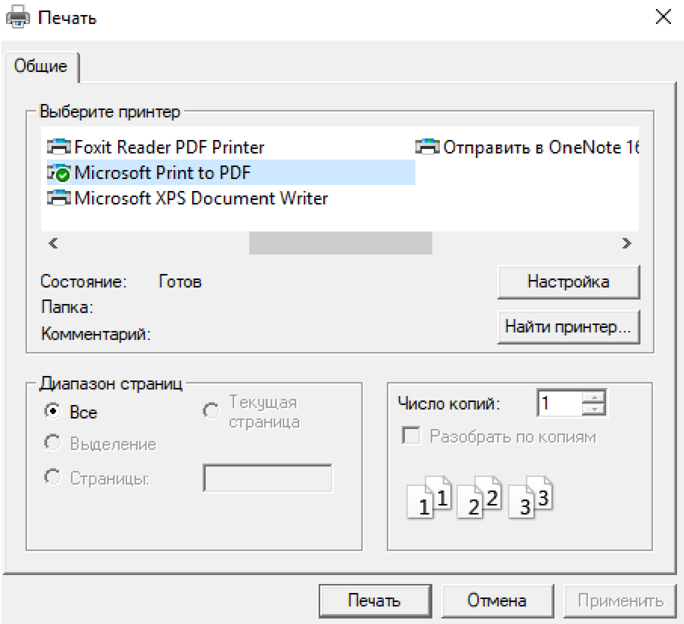


PrintPreviewWindow

Отчет

Текущий уровень угрозы: БВН

1.21 The preview mode of the report



Печать

Общие

Выберите принтер

Foxit Reader PDF Printer

Microsoft Print to PDF

Microsoft XPS Document Writer

Отправить в OneNote 16

Состояние: Готов

Папка:

Комментарий:

Диапазон страниц

● Все

○ Текущая страница

○ Выделение

○ Страницы:

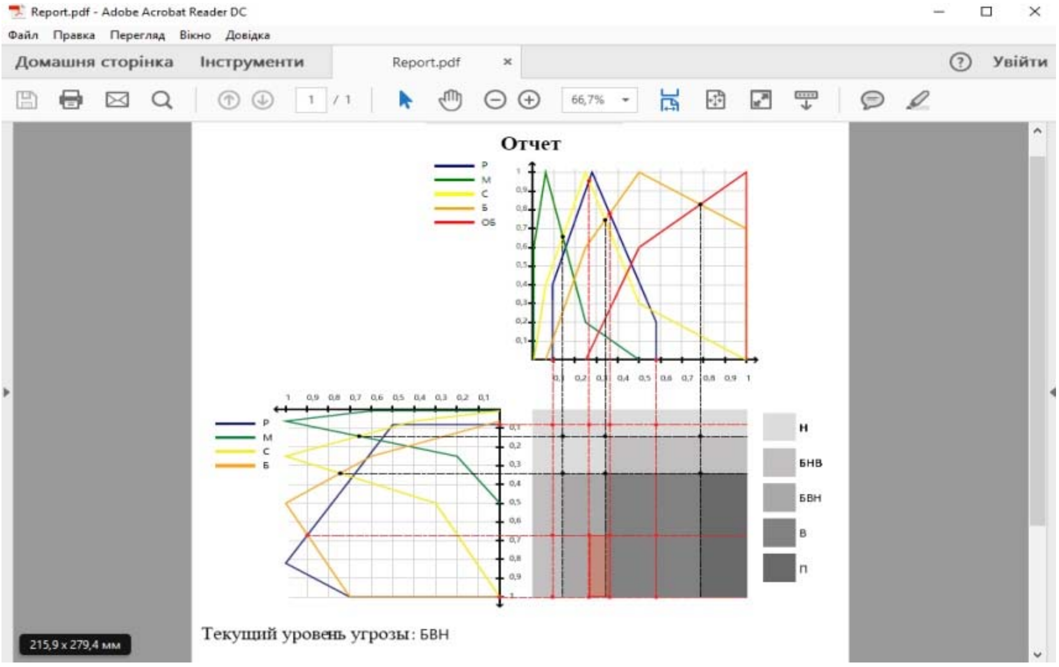
Число копий: 1

□ Разобрать по копиям

Figure 1.22 – Document Print Selection Window

The report also displays the equal anomalous state of the system (including at the moment of time).

Also, in the developed software there is used the Child Window module, which is responsible for the creation and editing of $\underset{\sim}{T}_{ijs}^{e}$ i $\underset{\sim}{P}_{ij}^{\tau_f}$ It is represented by a separate program window with a basic interface for performing the tasks created above. The data in the EDF can be modified and revised using the functionality of this module.



Текущий уровень угрозы: БВН

Figure 1.23 – Example of printing a report in pdf format

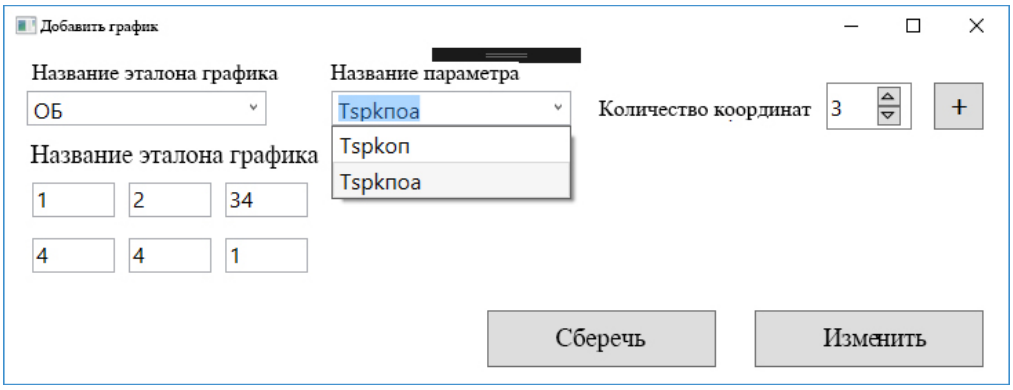
A similar procedure is implemented when the following buttons are activated:

- add;
- edit;
- delete.

Add a record (figure 1.24).

With the help of the "Add Graph" window functionality, you can add data such as:

- the name of the graphical image of the standard and current LF (selected using the ComboBox and the list of names)
- the amount and initialization of coordinate values (using “+” adds/extracts a new pair of coordinates is implemented).



[redacted]

Название эталона графика: ОБ

Название параметра: Tspknoa

Tspkon

Tspknoa

Количество координат: 3

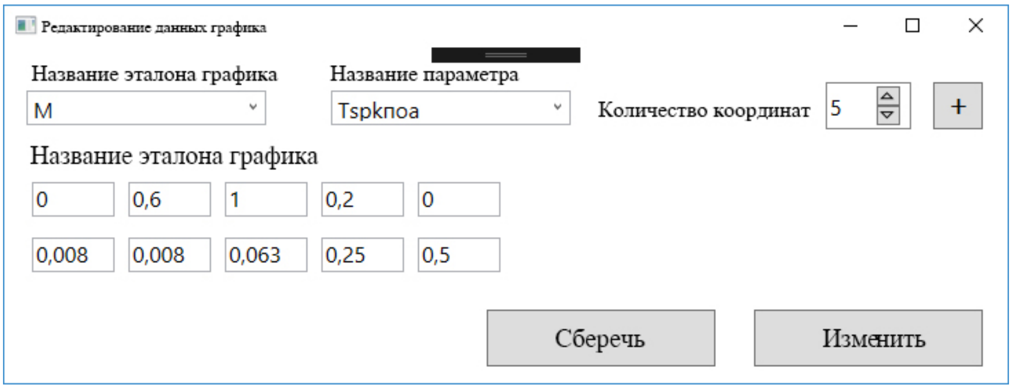
Название эталона графика

1	2	34
4	4	1

Figure 1.24 – Add Reference Values Record Window

The editing process is similar to the adding process, since the basis of the work of these procedures is similar. Therefore, after using the “Edit” button in the main window, a corresponding window appears where, using the “Edit Graph Data” functionality, you can modify it.

When you select the required line record to extract there is used the "delete" button, and the result is the extraction of data and its automatic update.



Редактирование данных графика

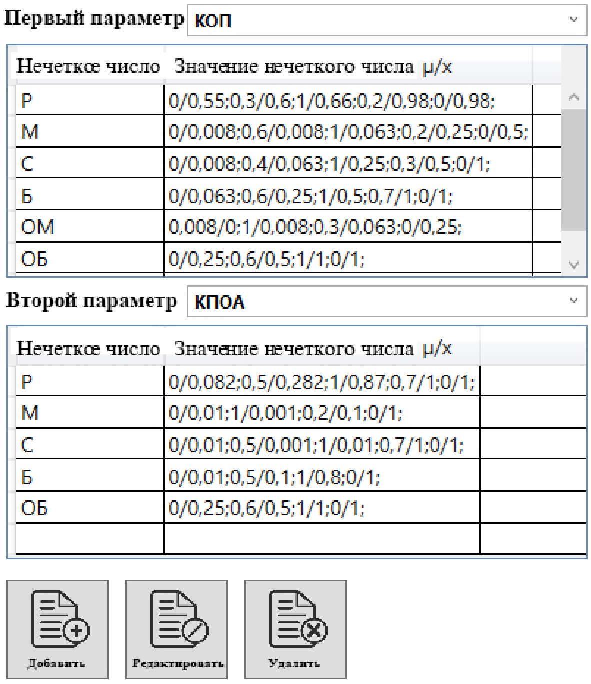
Название эталона графика: М

Название параметра: Tspknoa

Количество координат: 5

Название эталона графика

0	0,6	1	0,2	0
0,008	0,008	0,063	0,25	0,5



Первый параметр: КОП

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,55;0,3/0,6;1/0,66;0,2/0,98;0/0,98;
М	0/0,008;0,6/0,008;1/0,063;0,2/0,25;0/0,5;
С	0/0,008;0,4/0,063;1/0,25;0,3/0,5;0/1;
Б	0/0,063;0,6/0,25;1/0,5;0,7/1;0/1;
ОМ	0,008/0;1/0,008;0,3/0,063;0/0,25;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

Второй параметр: КПОА

Нечеткое число	Значение нечеткого числа μ/x
Р	0/0,082;0,5/0,282;1/0,87;0,7/1;0/1;
М	0/0,01;1/0,001;0,2/0,1;0/1;
С	0/0,01;0,5/0,001;1/0,01;0,7/1;0/1;
Б	0/0,01;0,5/0,1;1/0,8;0/1;
ОБ	0/0,25;0,6/0,5;1/1;0/1;

Figure 1.25 – Marking the line of the necessary record and its removal

Conclusions and statement of research objectives. Experimental research and practical use of the proposed software confirmed the formed theoretical positions, which became the basis of the developed algorithmic software. Therefore, the proposed software due to the basic algorithm and a set of developed procedures (construction of a coordinate grid; initialization of values based on a set of databases and modules; graphical formation of parameters; searching for common points according to basic rules and graphical interpretation of the result) [33, 34], automates the process of generating parameter standards for modern attack detection systems and reflects the results of the detection of an anomalous state in a given period of time. Also, the corresponding software can be used autonomously or, as an extender of the functionality of modern IDS.

Н. Жумангалиева[1], А. Досжанова[2], А. Корченко[3]

[1]Қ. И. Сәтбаев атындағы қазақ ұлттық техникалық зерттеу университет, Ақпарттық және телекоммуникациялық технологиялар институты, Алматы, Казахстан,
[2]IT-инжиниринг Алматинского университета энергетики и связи, Алматы, Казахстан,
[3]Ұлттық авиациалық университет, кафедра Ақпараттық технологиялар қауіпсіздігі, Украина, Киев

КИБЕРШАБУЫЛДАРДЫ ТАБУ ЖҮЙЕЛЕРІ ҮШІН ПАРАМЕТРЛЕР ЭТАЛОНДАРЫН ҚАЛЫПТАСТЫРУДЫҢ АЛГОРИТМДІК ЖӘНЕ БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУ

Аннотация. Жұмыста шабуылды анықтау жүйелері үшін алдыңғы зерттеулерге шолу және талдау жүргізілді және кибер шабуылдарды табу жүйелері үшін параметрлер эталондарын қалыптастырудың алгоритмдік және бағдарламалық қамтамасыз ету үшін жүйеде күдікті белсенділікті мониторингілеу және тараптың шабуылдау әрекеттерін анықтау үшін пайдаланылады. Кибершабуылдарды анықталмаған немесе анық емес қасиеттері бар кибер қауіпсіздердің жаңа немесе модификацияланған түрлері пайда болған кезде тиімді болып қала алатын арнайы техникалық шешімдерді жасауға бастамашылық етеді. Мұндай жүйелердің көпшілігі кибер шабуылдардың алдын алу бойынша тиісті шаралар қабылдау үшін күдікті белсенділікті немесе желіге араласуды анықтауға бағытталған. Шабуылды анықтаудың өзекті жүйелері болып табылады, олар аномалды жағдайларды сәйкестендіруге бағытталған, бірақ олар бірқатар кемшіліктерге ие. Бұл тұрғыда тиісті пән саласындағы мамандардың білімі мен тәжірибесін пайдалануға негізделген сараптамалық тәсілдер неғұрлым тиімді болып табылады. Сараптамалық тәсілдерге негізделген техникалық шешімдерді құру және арнайы құралдарды құру (мысалы, нашар қалыптасқан ортадағы анық Анықталған параметрлердің ағымдағы күйін бақылау арқылы бұрын белгісіз кибершабуылдарды анықтауға мүмкіндік беретін шабуылдарды анықтау жүйелері үшін бағдарламалық қамтамасыз ету) зерттеулердің перспективалық бағыты болып табылады. Кибершабуылдарды анықтаудың белгілі жүйесі негізінде, ол ауытқуыды (кибершабуылдардан туған) және тиісті әдістер мен модельдердің көптігін анықтау әдістемесіне негізделген ұсынылған бағдарламалық қамтамасыз ету, ол базалық алгоритм және бірқатар әзірленген рәсімдер (координат торының конструктивті; деректер базасы мен модульдер жиынтығы негізінде шамаларды инициализациялау; графикалық қалыптастыру; негізгі ережелерге сәйкес жалпы нүктелерді іздестіру және нәтижені графикалық интерпретациялау) шабуылдарды анықтаудың қазіргі заманғы жүйелері үшін өлшемдердің эталондарын қалыптастыру процесін автоматтандыруға және берілген уақыт аралығында аномалды күйдің детекторлау нәтижелерін көрсетуге мүмкіндік береді.

Түйін сөздер: кибершабуылдар; аномалиялар; басып кіруді анықтау жүйелері; шабуылдарды анықтау жүйелері; кибершабуылдарды анықтау жүйелері; ақпараттық жүйелерде аномалияларды табу.

Н. Жумангалиева[1], А. Досжанова[2], А. Корченко[3]

[1]КазНИТУ им. К. И. Сатпаева, Институт информационных и телекомминикационных технологии,
Алматы, Казахстан,
[2]IT-инжиниринг Алматинского университета энергетики и связи, Алматы, Казахстан,
[3]Национальный авиационный университет, кафедра Безопасности информационных технологий,
Киев, Украина

АЛГОРИТМИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ФОРМИРОВАНИЯ ЭТАЛОНОВ ПАРАМЕТРОВ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ КИБЕРАТАК

Аннотация. В работе проведен обзор и анализ предшествующих исследований для систем обнаружения вторжений, алгоритмическое и программное обеспечение формирования эталонов параметров для систем обнаружения кибератак

Системы обнаружения вторжений становятся неотъемлемой частью защиты любой сетевой безопасности, они используются для мониторинга подозрительной активности в системе и обнаружения атакующих действий неавторизованной стороны. Активизация кибератак инициирует создание специальных технических решений, способных оставаться эффективными при появлении новых или модифицированных видов киберугроз с неустановленными или нечетко определенными свойствами. Большинство таких систем направлена на выявление подозрительной активности или вмешательства в сеть для принятия адекватных мер по предотвращению кибератак. Актуальными системами обнаружения вторжений являются те, которые ориентированы на идентификацию аномальных состояний но они имеют ряд недостатков. Более эффективны в этом отношении являются экспертные подходы, основанные на использовании знаний и опыта специалистов соответствующей предметной области. Построение технических решений и создание специальных средств (например, программного обеспечения для систем обнаружения атак, позволяющих детектировать ранее неизвестные кибератаки путем контроля текущего состояния нечетко определенных параметров в слабоформализованной среде) основанных на экспертных подходах, является перспективным направлением исследований. На основе известной системы обнаружения кибератак, которая базируется на методологии выявления аномалий (порожденных кибератаками) и множества соответствующих методов и моделей предложенное программное обеспечение, которое, за счет базового алгоритма и ряда разработанных процедур (координатной сетки; инициализации величин на основе набора баз данных и модулей; графического формирования параметров; поиска общих точек согласно базовых правил и графической интерпретации результата) позволяет провести процесс формирования эталонов параметров для современных систем обнаружения атак и отражать результаты детектирования аномального состояния в заданный промежуток времени.

Ключевые слова атаки; кибератаки; аномалии; системы обнаружения вторжений; системы обнаружения атак; системы обнаружения кибератак; обнаружение аномалий в информационных системах.

Information about authors:

Zhumangaliyeva Nazym, PhD student, Kazakh National Research Technical University after K. I. Satpayev, Almaty, Kazakhstan; nazym_k.81@mail.ru; https://orcid.org/0000-0003-1130-3405

Doszhanova Aliya, Almaty University of Power Engineering and Telecommunications, Kazakhstan, PhD, Associate professor; d_alia.81@mail.ru; orcid.org/0000-0002-6932-6282

Korchenko Anna, National aviation University, Kyiv, Ukraine; Department of information technology Security, candidate of technical Sciences, associate Professor; annakor@ukr.net; orcid.org/0000-0003-0016-1966

REFERENCES

[1] A. Korchenko, V. Shcherbina, N. Vishnevskaya, "Methodologybetween systems for detecting anomalies generated by cyberattacks", zahist nformats, Vol. 18, no. 1, Pp. 30-38, 2016.

[2] A. Korchenko, Would. Akhmetov, V. Shcherbina, P. Vikulov, "Structural-analytical model metodologiyasini systems villeneuvette", the Status and improving the security of information technology systems (SITS`2017): 9-and SEUK. sciences'.-prakt. Conf., Koblevo, Mykolaiv region, 2017, p. 42-44.

[3] A. Korchenko, "Tuple model of formation of a set of basic components for the identification of giberatak", Legal, regulatory and metrological support of the information security system in Ukraine, V. 2 (28), Page. 29-36, 2014.

[4] A. Korchenko, "the Method of formation of linguistic standards for villeneuvette", information, vol. 16, no. 1, Pp. 5-12, 2014.

[5] V. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, "Improved method for the formation of linguistic standards for of intrusion detection systems", Journal al of the oreticaland applied information technology, vol. 87, No. 87. 2, pp. 221-232, 2016.

[6] I. Traykovski, A. Korchenko, P. Vikulov, I. Rafg, "Model standards of linguistic variables for detecting email spoofing-attacks", information Security. Vol. 24, No. 2, Pp. 99-109, 2018.

[7] A. Korchenko, N. Gumargalieva, P. Vikulov, " Construction of linguistic standards for viewlegislation attacks," Topical problems in the provision of cyber security and information protection: III Intern. sciences'.-prakt. Conf., Kiev, 2017, Pp. 93-97.

[8] A. Korchenko, " Formation of linguistic standards on snow continuous for villeneuvette", the Status and improving the security of information technology systems (SITS`2015): 7-and SEUK. sciences'.-prakt. Conf., the village of Koblevo Nikolaev obl., 2015, P. 43-46.

[9] M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, "The Etalon Models of LinguisticVariables forsniffing-AttackDetection", inIntelligent Data Acquisition and Advanced computing systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conferenceon, 2017, pp. 258-264.

[10] A. Korchenko, "the Method of possibilitiesyou on lingvisticheskaja for viewingaccelerating" information Security, vol. 20, no. 1, Pp. 21-28, 2014.

[11] N. Karpinski, A. Korchenko, S. Kazmirchuk, "Possibilitypomeroy in continuemodal for viewingaccelerating", the Status and improving the security of information technology systems (SITS`2016): 8-and SEUK. sciences'.-prakt. Conf., the village of Koblevo Nikolaev obl., 2016, P. 39-42.

[12] A. Korchenko, "Method -uravnoveshinaya numbers for obnaruzhiteli", information, vol. 16, No. 4, Pp. 292-304, 2014.

[13] N. Karpinski, A. Korchenko, P. Vikulov, N. Gumargalieva, "Nominalistically values for syavleniyami", Sovremennikami and kommunikations technologie transport, industry and education (TEMPUS: CITISET): X Intern. science.-prakt. Conf., Dnipro, 2016, Pp. 51-52.

[14] A. Korchenko, "Method of identification of identification terms for detection systems of rejection", information Security, Vol. 20, №3, Pp. 217-223, 2014.

[15] A. Korchenko, "the Method of definitions of identifying terms for viewingaccelerating" Relevant issues of ensuring of cyber security and protection of information: scientific.-prakt. Conf., Kyiv, 2015, Pp. 64-67.

[16] N. Karpinsky, A. Korchenko, S. Akhmetov, "Method of formation of base detection rules for detection systems", information Protection, Vol. 17, №4, Pp. 312-324, 2015.

[17] N. Karpinski, A. Korchenko, Akhmetov, N. Gumargalieva, "the Method of construction of conditional detection expressions for baruunkharaa" Relevant issues of ensuring of cyber security and information protection: II Intern. sciences'.-prakt. Conf., Kyiv, 2016, Pp. 65-69.

[18] A. Korchenko, Z. Alimseitova, N. Zhumangaliyeva, "A system for identifying anomaly state informational systems", in Inżynier XXI Wieku: VII Międzynarodowa Konferencja student woraz doktorantow, 08.12.2017: monografia, 1st ed., Vol.2., Bielsko – Biała (Poland): AkademiaTechniczno- Humanistyczna w Bielsku-Białej, 2017, pp. 39-48.

[19] M. AlHadidi, Y. Ibrahim, V. Lakhno, A. Korchenko, A, Tereshchuk, A. Pereverzev,"Intelligent systems form on itorin gandre cognition of cyberattacks on information and communication systems of transport", International Reviewon Computers and software (IRECOS), vol. 11, No. 2, pp. 1167-1177, 2016.

[20] A. Korchenko, "System formation of fuzzy standards of network parameter ",. Vol. 15, No. 3, Pp. 240-246, 2013.

[21] A. Korchenko, "System farmerbeneficiaries to identify suspicious activity ", Integrated intelligent robotic systems (RD-2014) : VII Intern. sciences'.-prakt. Conf., Kiev, 2014, P. 354-355.

[22] "Basic features of classification systems obnaruzhiteli", Sovremennikami-telekommunikations technologie]. science.-tech. Conf., Kazakhstan, GUT, 2015, Pp. 24-26.

[23] S. Kazmirchuk, A. Korchenko, T. Parashchuk, "analysis of intrusion detection systems", information protection, vol. 20, №4, Pp. 259-276, 2018.

[24] I. Traykovski, A. Korchenko, T. Parashchuk, Is. Pedchenko, "Analysis of open intrusion detection systems", information Security. Vol. 24, No. 3, Pp. 201-216, 2018.

[25] I. Traykovski, A. Korchenko, "System view ingaccelerating" information Security, vol. 23, no. 3, Pp. 176-180, 2017.

[26] A. Korchenko, S. Kazmirchuk, V. Shcherbina, P. Vikulov, " Expander functionality for obnaruzhiteli" Relevant issues of ensuring of cyber security and information protection: IV international. sciences'.-prakt. Conf., Kiev, 2018, P. 78-80.

[27] A. Korchenko, A. Zaritsky, T. Parashchuk, V. Bychkov, "Software for the formation of standards of parameters for cyberattack detection systems", information Protection. Vol. 20, No. 3, Pp. 133-148, 2018.

[28] Akhmetov BS, Gnatyuk S., Zhmurko T., Kinzeryavyy V., YubuzovaKh.(2018) Experimental research of the simulation model for deterministic secure communication protocol in quantum channel with noise // Reports oft henational academy of sciences of the republic of kazakhstan, ISSN 2224-5227, Volume 5, Number 321 (2018), 5 – 11. DOI:https://doi.org/10.32014/2018.2518-1483.1 (InEng)

[29] Software module for formation of parameter standards for anomaly detection systems. Computer program / T. Parashchuk, A. Korchenko – K. – Certificate of registration of copyright in the work №74016 from 02.10.2017.

[30] A. O. Korchenko, There Is.V. Ivanchenko, V. V. Pogorelov " "evaluation of the effectiveness of the expert system of intrusion detection based on fuzzy logic", Scientific notes of TNU named after V. I. Vernadsky. Series: technical Sciences, vol. 30 (69), №1, Pp. 66-72, 2019.

[31] Bugubayeva RO., Tapenova GS., **(2019)** Regulatory aspects of public administration system of higher education in the republic of kazakhstan//Bulletin of national academy of sciences of the Republic of Kazakhstan. ISSN 2224-5294 Volume 1, Number 323 (2019), PP.151-160. https://doi.org/10.32014/2019.2224-5294.24 ISSN 2224-5294 (Online),

[32] Seitmuratov A., Zharmenova B., Bekmuratova A.K., Tulegenova E., G. Ussenova.**(2018)** Numerical analysis of the solution of some oscillation problems by the decomposition method// Bulletin of national academy of sciences of the Republic of Kazakhstan. Volume 1, Number 323 (2019), P.28-37. https://doi.org/10.32014/2019.2518-1726.4 ISSN 1991-346X (Online), ISSN 1991-3494 (Print).

[33] Suiekpayev Y., Sapargaliyev Y., Bekenova G., Kravchenko M., Dolgopolova A., Seltmann R. **(**2018) Organization of computer laboratory work calculation and visualization of small forced oscillations// Bulletin of national academy of sciences of the Republic of Kazakhstan. Volume 3, Number 430 (2018), P.145-154. https://doi.org/10.32014/2019.2518-170X.1 ISSN 2224-5278 (Online)

[34] Sarsenov A.M., Bishimbayev V.K., Kapsalyamov B.A., Lepessov K.K., Gapparova K.M. (2018) /Interphase distribution of boric acid between aqueous solutions and modified cellulose// Bulletin of national academy of sciences of the Republic of Kazakhstan. Volume 6, Number 376 (2018), P.34-38. https://doi.org/10.32014/2018.2518-1467.24 ISSN 1991-3494(Online)

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/en/

Редакторы *М. С. Ахметова, Т. М. Апендиев, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 13.12.2019.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
23,2 п.л. Тираж 500. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19