ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 1, January 2019

Algorithmic model of protecting information systems based on operating tables

Kabulov Anvar Vasilovich, Varisov Akmal Abbasovich, Karimov Anvar Abdivokhidovich

ABSTRACT: The article proposes one of the ways to analyze the security of a system - the construction of dynamic tables of functioning (TF) of an information system. With the help of the TF-based algorithmic model, the functioning of the implemented protection system is examined and its drawbacks are revealed. In the work, algorithmic models based on TF are used as a mathematical apparatus for modeling dynamic discrete systems.

KEYWORDS: information system, information security, risk assessment, threats, methods, table of functioning, probability, flow, confidentiality, information, damage, audit, synthesis, identification.

I. INTRODUCTION

One of the ways to analyze the security of a system is to build dynamic tables of functioning (TF) information systems [1]. With the help of the algorithmic model based on the TF, the functioning of the implemented protection system is examined, and its drawbacks are revealed. Algorithmic models based on TF [1,2] are used as a mathematical apparatus for modeling dynamic discrete systems, providing comprehensive protection of information systems (IS) against all external and internal threats for a given logical sequence. The algorithmic model for ensuring integrated protection of IS consists of several main parts:

1. General structural model for ensuring security of IP based on the table of functioning;
2. A mathematical model for identifying threats from external and internal sources;
3. Synthesis and analysis of the construction of the table of functioning after obtaining the necessary data at the stage of «SYNTHESIS».
4. Ways, methods, methods, models and means of destruction of detected threats. Here you can also get information about the destruction of the sequence of detected threats in the table of functioning as a graph. Paths of threat destruction are displayed in the chains of the graph;
5. Analysis of possible threats to the information system, risk analysis and analysis of the security of information systems.

II. GENERAL STRUCTURAL MODEL FOR ENSURING SECURITY OF AN IP BASED ON A FUNCTIONING TABLE

The presented model has three different ways to solve the problem in order to provide a comprehensive information protection system (CIPS). The first is that if the threat was previously considered and studied, then after the "General Archive (R + I) viewed threats" stage, the threat proceeds to the "Neutralize $P_{ij}F$ threats" stage and the threat is completely destroyed. In this case, it is possible not to use the wide possibilities of the functioning table (Fig. 1 "a").Secondly, if the threat has not been previously considered and has not been studied, then the second way to solve the problem will be used. But at the same time, this type of threat and possible concrete actions to eliminate this threat are known and they are displayed in the O'zDSt 2927: 2015 standard - the State Standard of the Republic of Uzbekistan "Information technology, information security, terms and definitions". After the stage "General archive (R + I) of viewed threats", it is necessary to proceed to the action and solution of the problem with the help of the TF and obtain various sets of values "Analysis and calculation of Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i". After that, the system consistently collects the necessary information in stages. These are "Analysis of the source of threats Y+Z", "Analysis of the privilege of threats Z_k", "Revision of threats $Y+Z_k$", "Archive of missed threats (P)" (Fig. 1 "a").

When all the steps of the second path of the algorithmic model of the TFZ-based security security model will be considered, then all these steps are repeated starting from the "O_j Threat Identification" stage. If, in the re-examination, threats are identified as previously known, then the action to eliminate the threat will occur in the first way to ensure the CIPS.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

Thirdly, if the threat has not been previously detected and is unique in its structure to provide the CIPS. A special feature of this method is the fact that all threats that are not included in the O'zDSt 2927: 2015 standard - the State Standard of the Republic of Uzbekistan «Information technology, information security, terms and definitions» (Fig. 1 «a»), Fig. 1 «b»).

After the stages "General archive (R+I) of the threats viewed" and "Analysis and calculation of Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i", the calculations and analysis proceed successively to the stages "Adding a function and definition", "Adding initial inspection information", "Threat Source Analysis", "Threat Privilege Analysis", "Threat Revision", "Archive of Modified Threats (I)". After going through all the steps in the third way to ensure the CIPS, the next steps will be the "O_j Threat Identification" stage.

Presented in Fig. 1 «a», fig. 1 «b» each stage/unit has its own specific actions and functionality.

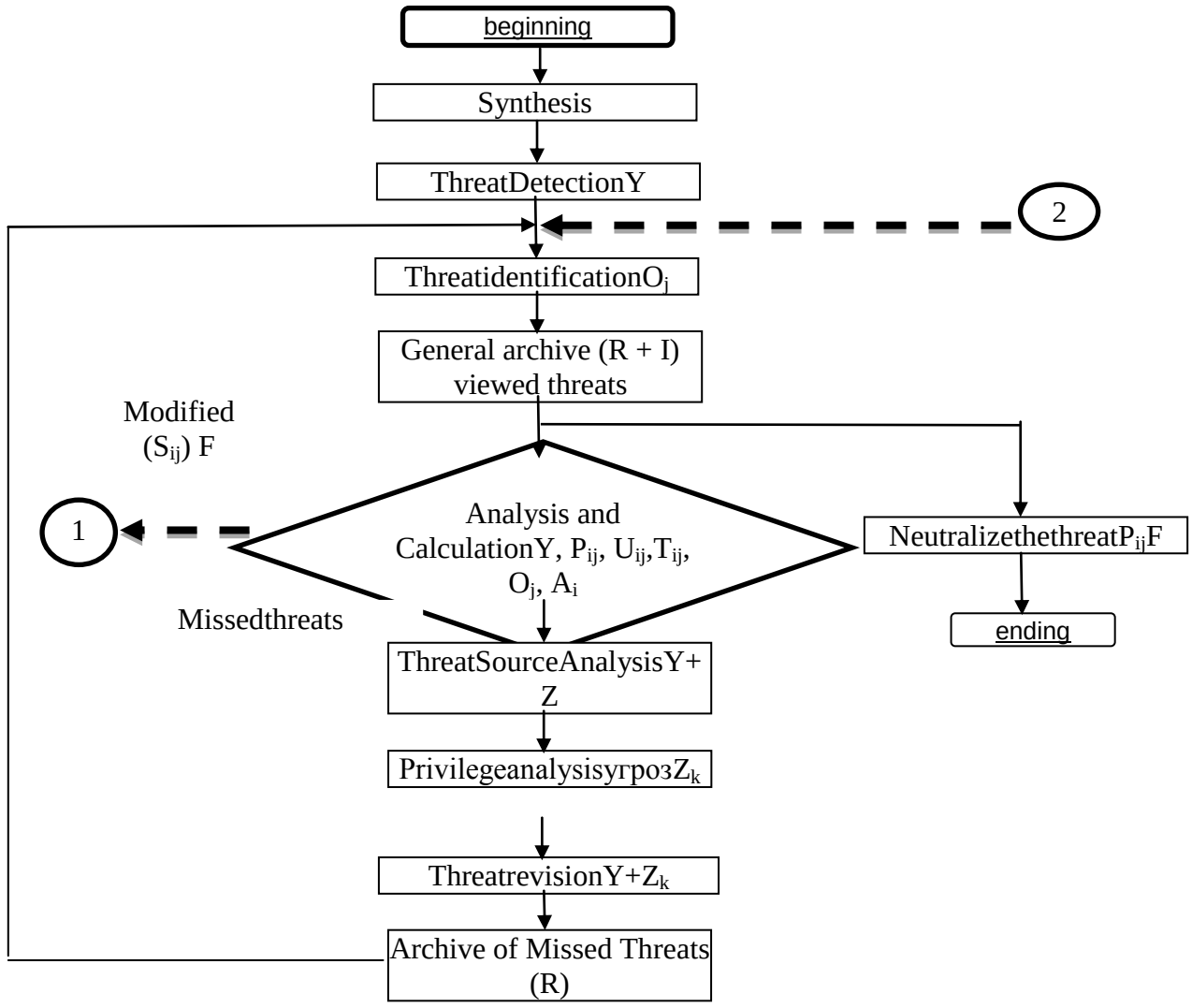

Fig. 1 «a» Algorithmic model of ICF based on TF

The first step of the algorithmic model CIPS is «Synthesis». At this step, the system analyzes the received information, streams, packets and their sources. Based on the received data, the system activates the necessary panels to ensure the security of the IC.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 1, January 2019

TF includes several stages (Fig. 1 “a”) consisting of “Identification of O_j threat”, “Analysis and calculation of Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i”, “Neutralize threats of $P_{ij}F$”, “Analysis privileges of Z_k threats”, etc. The remaining stages that are not included are analytical, additional information and databases of the threats studied.

III. SYNTHESIS AND ANALYSIS OF THE CONSTRUCTION OF THE TABLE OF FUNCTIONING AFTER OBTAINING THE NECESSARY DATA AT THE STAGE OF «SYNTHESIS»

Building a security system is imperative to ensure the security of confidential information stored and processed in an information system. Information protection system requirements are formed based on the results of the information system survey and are focused on neutralizing system vulnerabilities. One way to analyze the security of a system is to build dynamic TF information systems based on Petri nets [3]. With the help of an algorithmic model based on the TF, an examination of the functioning of the implemented protection system is carried out, and its drawbacks are revealed. In the development of the TF, an ideological model of the Petri net was chosen. In the algorithmic model CIPS after “Start”, the main steps are “Synthesis”. In this step, the system analyzes the received information, streams, packets and their sources. Based on the data obtained, the system activates (or builds) the necessary panels to ensure the security of the IS.

After receiving at the first stage signals, packets, all sorts of information, the algorithm of the CIPS begins to function. At the second stage of the Synthesis algorithm, the CIPSseparates the received streams into two types:

1. Trust information.
2. Suspicious information.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

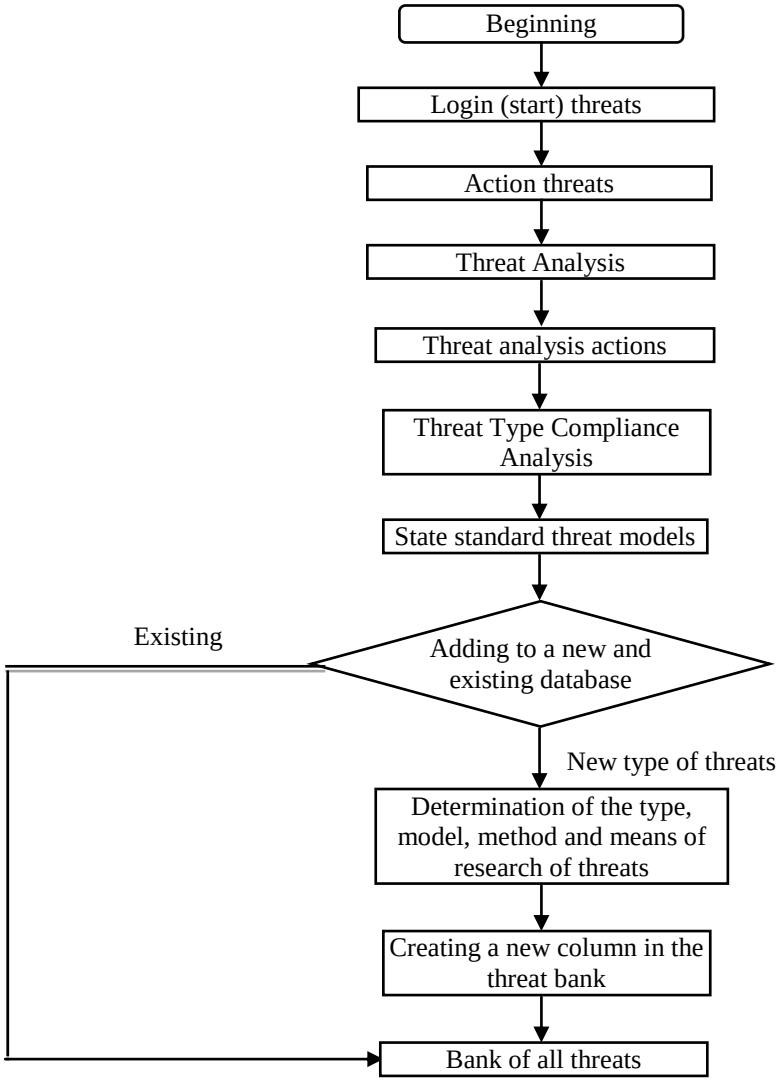

Fig. 2. Algorithmic model of threat identification.

The scheme of work on the second stage is presented in Figure 3.

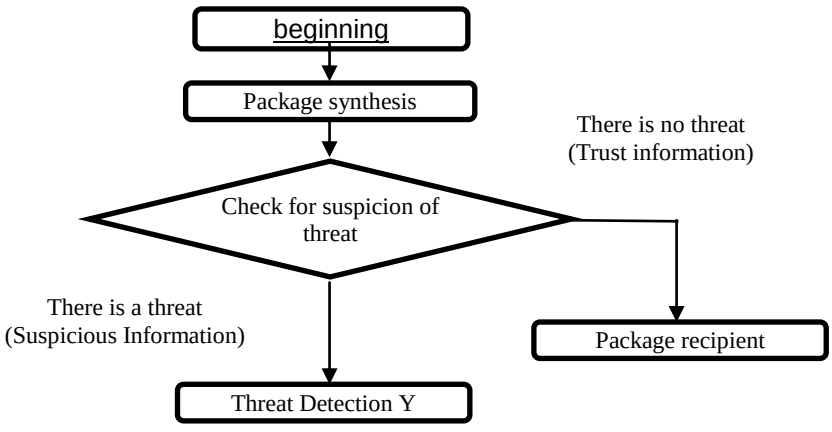

Figure 3. Synthesis of incoming packets

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

Checked packages without detected suspicions are sent to the recipient of information in the prescribed manner. Packages with detected suspicions of the threat are sent in the third block of Fig. 1 “a”, “Detection of threats Y”. A suspicion check will be carried out in the database on the main criteria and signs of threats as follows:

a. Analysis of the required area in the TF for the destruction of the threat.
b. Construction of the necessary area of TF.

IV. WAYS, METHODS, METHODS, MODELS AND MEANS OF ELIMINATING DETECTED THREATS.

Consider the ways, methods, methods, models and means of destruction of detected threats. Here you can get information about the sequence of the destruction of detected threats in the table of functioning in the form of a graph, where the ways of destruction of threats are displayed. The TF data was obtained from the O’zDSt 2927: 2015 standard - the State Standard of the Republic of Uzbekistan “Information technology, information security, terms and definitions”. All listed in this standard are information security management, information security, information security threats, risks, attacks, information protection methods, cryptographic methods of information protection, protection of sensitive information, information protection tools, information security of telecommunications networks, information security of mobile communications, protection and data recovery, copy protection and others are distributed in the TF according to the characteristics and logical performance of actions by them. For example, in the table of functioning of the CIPS (Fig. 4), the first upper line contains the terms and definitions of information security threats, risks, and attacks in the form of classes .One class Y-the set of possible threats O_j ($Y = \{O_j\}$), can contain many varieties of various threats, combined according to the criteria and actions of the threats in question.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

A_X \ O_Y	O_1	O_2	O_3	…	O_j
A_1					
A_2					
A_3					
…					
A_{i-1}					
A_i \ Z_k	Z_1	Z_2	Z_3	…	Z_k

Fig. 4 Table of operation of CIPS

Similarly, the first column of the table of CIPS operation (Fig. 4) presents the means, methods and models for ensuring the security of information technologies of typical organizations, enterprises and institutions (X is the set of threat prevention solutions A_i (X = {A_i}). For example, A_i-authorization, discretionary access control, access control policy, list of authorities, access subject, security zone, multi-level protection, closed secure environment, obstacle, regulation, shielding, encryption, antivirus program, computer audit computer system, fault tolerance, manipulation detection, control of keystrokes, emergency procedures, etc.

The last bottom line of the TF presents Z - many privileges. This can be all sorts of administrator privileges, users, as well as the system itself. Studying with which privileges the threats entered into the system of VETS, the choice is made by what methods and means to ensure protection against this threat.

In addition to the above, the TF also calculates all possible risks that threaten the efficiency of the IP, as well as the risks of losing the value of information in the system. Based on the obtained results, when studying risks from possible threats, the system identifies the vulnerabilities in the system and suggests possible steps to improve the quality of security of the CIPS.

In the TF, while ensuring security and studying the risks of countering threats, the ways of possible and real threats are displayed in the form of graphs (Fig. 5). This gives an objective approach to the consideration and study of each threat separately.

On the basis of the TF CIPS, it is possible to get answers and ready-made solutions on a variety of questions and requirements of the state standards of the republic while ensuring the security of information systems. For example, the TF implements answers to the requirements of the tasks of the standards O'zDStISO/IEC 27000: 2014

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

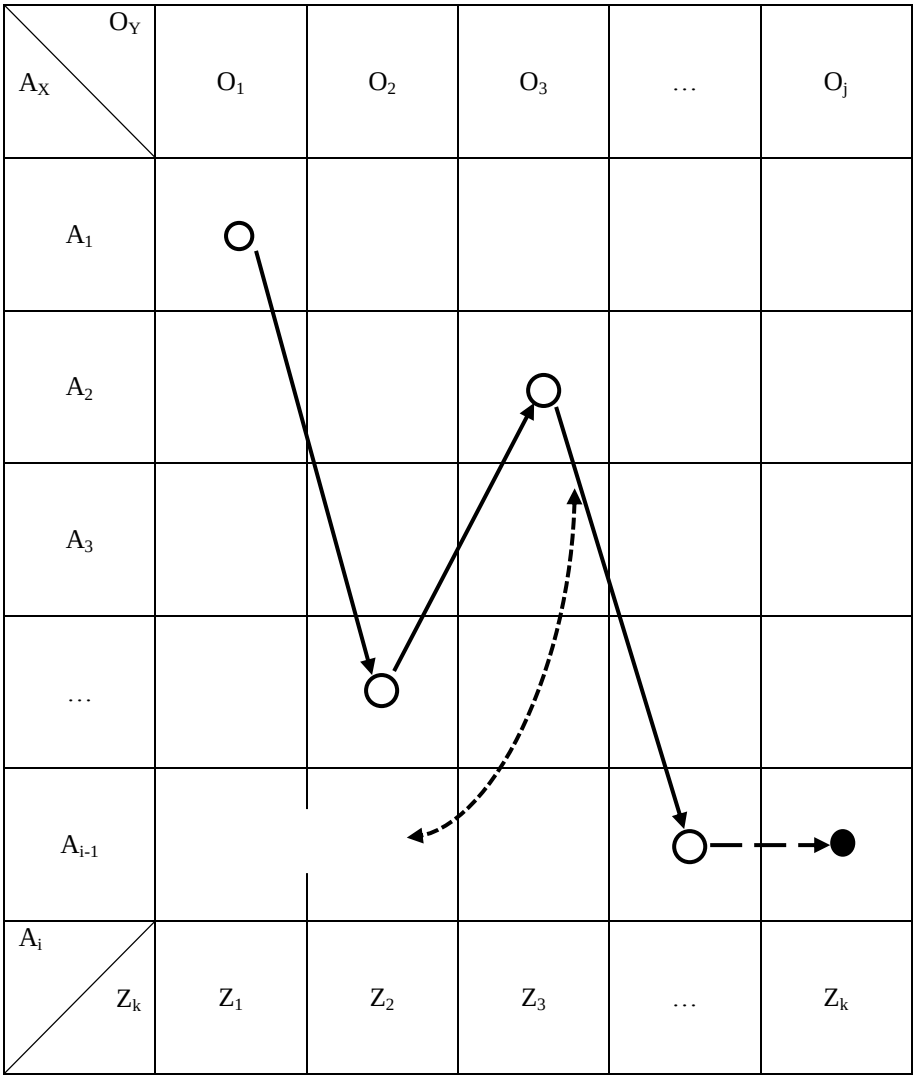

Fig. 5. The table of the functioning of CIPS

State Standard of the Republic of Uzbekistan "Methods of ensuring security. Information Security Management Systems", O'zDStISO/IEC 27035: 2015 MOD State Standard of the Republic of Uzbekistan "Security Management Methods. Information Security Incident Management", O'zDStISO/IEC 27004: 2014 State Standard of the Republic of Uzbekistan "Security Management Methods. Measuring the effectiveness of the information security management system", O'zDStISO/IEC 27005:2013 State standard of the Republic of Uzbekistan "Information technology. Security methods. Information Security Risk Management, etc.

In the development of the TF, an ideological model of the Petri net was chosen. Building a security system is imperative to ensure the security of confidential information stored and processed in an information system. Information protection system requirements are formed based on the results of the information system survey and are focused on neutralizing system vulnerabilities. One way to analyze the security of a system is to build dynamic TF information systems based on Petri nets. With the help of an algorithmic model based on the TF, an examination of the functioning of the implemented protection system is carried out, and its drawbacks are revealed.

One of the main features of the TF is the identification of threats to distribute it according to criteria and characteristics that have negative effects on the system. In this case, previously unknown threats after scanning are

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

compared by already known classes of threats. If the threat is unique to it in the TF, a separate cell is allocated, otherwise this threat is added to the most appropriate classes of threats.

The above algorithm works on TF displays the sequence of functioning of the TF as a whole. But in each cell there will be other algorithms and other tasks to ensure the security of information systems.The descriptions of these actions are represented by the formula θij = {Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i, Z_k}. Here TF={X,Y,A,O,Θ,T,U,S,F,P} is an algorithmic model of the automatically system managementfor ensuring the security of IS, as well as preventing any kind of threats to IS and information resources (IR), where Y is the set of possible threats O_j(Y={O_j}); X is the set of solutions for threat prevention A_i (X = {A_i}); A is a specific threat prevention solution; O- a certain action of threats; Θ - coordinates between «A_i» and «O_j»; T-time to prevent and successfully implement a threat; U-external influence on the coordinate Θ_{ij} on {Ai: O_j}; S is the set of transitions (transition from one Θij to another Θ_i + n, j + m); F(t) is the function of changing the table of functioning in time; P is a set of computational and logical input, output and control operations; Z - a lot of privileges.
analyze

V.ANALYSIS OF POSSIBLE THREATS TO THE INFORMATION SYSTEM, RISKS AND SECURITY OF INFORMATION SYSTEMS

$$V_1 = \text{Analyze}\{P^{internet} + D\} V_2 = \text{Analyze}\{P^{local.net} + D\} V_1 = \text{Analyze}\{D\},$$

Where P – program, D – action and analysis = {the frequency and source of the update, the execution time of the actions, the sending}

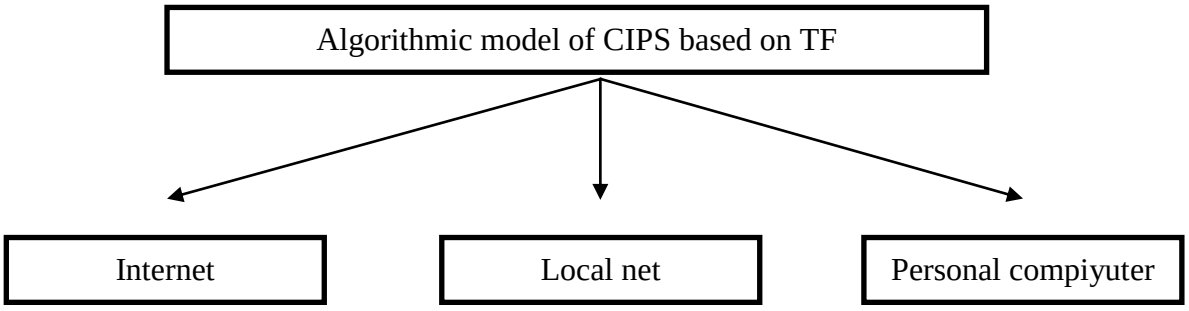

Fig. 6. Algorithmic model of CIPS based on TF

The way to build an information security management system (ISMS) in an organization depends on the presence of categorical information in it.

The requirements for the risk assessment methodology are the following: the effectiveness of applying the obtained results to create an ISMS, an acceptable amount of input data, and uniquely interpretable output results.

VI. CONCLUSION

The risk of the realization of at least one threat from the entire list of actual threats, taking into account the presence of vulnerabilities in relation to a competitive asset, is determined by the general formula:

$$R = R_{угр} * R_n * C_x \frac{K_o + K_t}{2} * 100\%, \quad где$$

R is the numerical value of the risk of realization of IS threats;
Rug - the probability of the realization of at least one threat from the entire list of actual threats;
Rn - the risk of non-compliance with legal requirements;
C - asset value;
Ko is the probability of exploiting organizational vulnerabilities;
Kt is the probability of exploiting technical vulnerabilities.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

Numerical data and their graphical display are given in table 1 and in figure 8.

Table 1

R	3281250000000	18975000000000	25200000000000	21280000000000
$R_{(yrp)}$	50	60	80	40
R_n	35	46	90	80
C_x	1500000	2500000	1000000	1900000
K_o	15	25	20	50
K_t	10	30	50	20

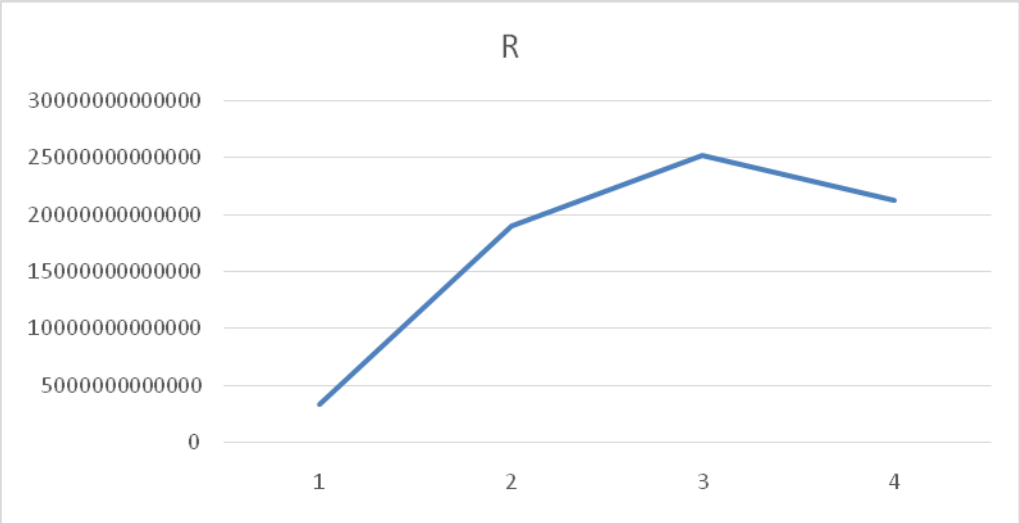

Fig.8. Graphic display of risk.

Here, if solutions come out with positive values, then P shows how many percent of the threats pass through the defense of the CIPS. If solutions come out with negative values or with zero scores, then protection is fully secured. According to this formula, it is possible to easily calculate the percentage of resistance of the CSID. But there are other ways to calculate the information security system. Let R be the possible risk of CIDP and analysis; Y is the set of possible threats Oj; P - the probability of the threat.The probability of a threat is calculated from the functioning table, with all possible existing threats being divided according to certain scales. When attacking information systems, the greater the value of P, the greater the damage from such an attack. Possible risk is calculated using the following formula:

Let Y be the set of possible threats Oj, Y = {Oj}, X is the set of solutions for Ai to prevent threats, X = {Ai}, P is the percentage of the possible risk of CIPF, then

$$P = \frac{X\{Ai\} - Y\{Oj\}}{Y\{Oj\}} * 100.$$

Here, if solutions P have positive values, then R shows how many percent of the threat passes through the defense of the CIPP.

The likelihood P of a threat is calculated from the functioning table, with all possible existing threats being divided according to certain scales. When attacking an information system, the greater the value of P, the greater the damage from this attack. The risk is calculated in the following ways:

$$R = A * P.$$

If we combine the first and second formulas, then we get:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 1, January 2019

$$R = A * \frac{X\{Ai\} - Y\{Oj\}}{Y\{Oj\}} * 100.$$

The numerical data and their graphic display are given in table 2 and in figure 9.

Table 2

R	400	-750	1666,667	625
A	20	60	10	50
X {Ai}	60	70	80	90
Y {Oj}	50	80	30	80

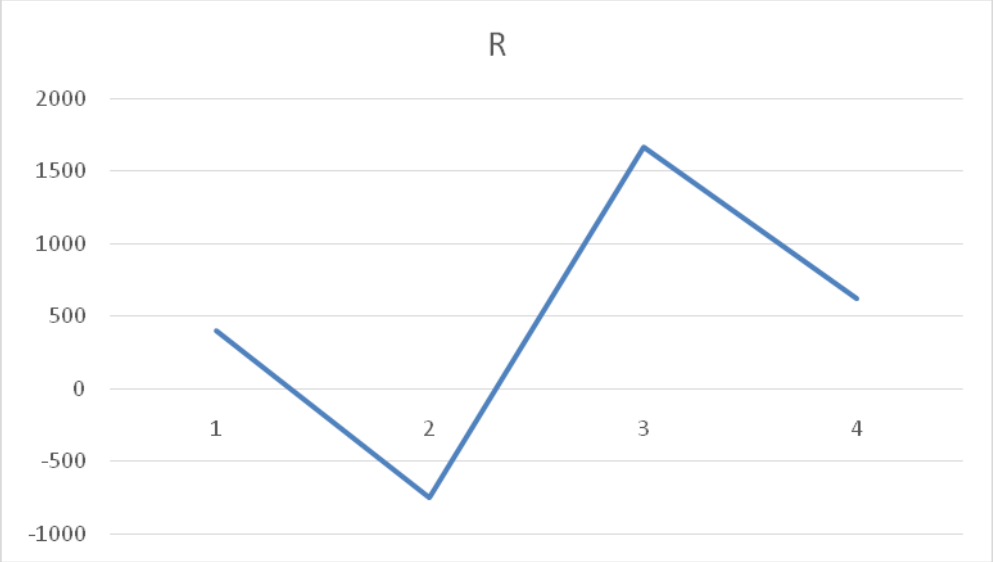

Fig.9. Graphic display of risk magnitude.

Thus, the paper proposes the construction of an algorithmic model of an ICF for the study of complex information systems based on functioning tables. From the point of view of information security, algorithmic models based on TF are used as a mathematical tool for modeling dynamic discrete systems.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 1, January 2019

REFERENCES

1. A.V.Kabulov, A.Varisov. Algorithmic models of information security based on the tables of functioning International Journal of Science and the World. № 6,2017, vol1.

2. A.V.Kabulov, A.Varisov. Algorithmic models of information security based on dynamic tables of functioning. Fundamental and applied research. Sat articles of the winners of the international scientific conference. Penza. 2017

3. J.Peterson. The theory of Petri nets and modeling systems. - M.: Mir, 1984.

AUTHOR'S BIOGRAPHY

A.V. Kabulov, Professor of the Department of the National University of Uzbekistan named after Mirzo Ulgbek, Doctor of Technical Sciences. Author of more than 100 scientific papers.
A.V. Kabulovwas engaged in the study of information technology, information security and mathematical modeling of processes of action.

A.A.Varisov Scientific applicant of the Tashkent University of Information Technologies, chief specialist of the Development Center of "Electronic Government". Author of more than 15 scientific papers.
A. A. Varisov is assistant professor of Computer Science. He has been a practicing Educational Consultant for Information Security, E-Government, evolution funded projects of ERASMUS MUNDUS, With Security organizations, with university's and many companies. His current research interests include orchestrating framework in cloud computing, data mining.

KarimovA.A. Scientific applicant of the National University of Uzbekistan named after Mirzo Ulgbek of the Republic of Uzbekistan, Head of the Department of Information and Communication Technologies. Author of more than 10 scientific papers.
Karimov A.A. engaged in information technology, information security and information process modeling.