Bulletin of TUIT: Management and Communication Technologies

Volume 2 Article 2

8-12-2019

Model of the state of threats to the Access Control System

Durdona Irgasheva
"Bulletin of TUIT: Management and Communication Technologies", ab.shaxnoza84@gmail.com

Ganiev S.K., Irgasheva D.Y.

Model of the state of threats to the Access Control System

Abstract. This article is devoted to the presentation of the threat state model of access control, which allows calculating the probabilities of the impact of threats on the access control system and the probability of opening this system based on taking into account the generalized algorithm for the implementation of external threats, and determines the need to develop additional components of the access control system designed to identify and classify attacks.
Keywords: Computer system, threats, attacks, access control system, model, state, hacking.

Introduction

The organization for ensuring information security should be comprehensive. It should be based on a deep analysis of all kinds of negative consequences. Analysis of negative consequences implies the mandatory identification of possible sources of threats, factors contributing to the emergence of vulnerabilities and, as a consequence, the identification of actual threats to information security. An access control system is an interconnected set of heterogeneous means that protect computer systems from unauthorized access to information. Delimitation of access to information - the division of information circulating in computer systems into parts, elements, components, objects, etc. and the organization of a system for working with information, involving users' access to those components of information that they need to perform their functional duties or is necessary based on other considerations [1].

Main part

The access control system is one of the main components of an integrated information security system. In this system, the following components can be distinguished:

- means of authentication of the access subject;
- means of delimiting access to technical devices of a computer system;
- means of differentiating access to programs and data;
- means of blocking illegal actions;
- means of registration of events;
- the operator on duty of the access control system.

Based on the types of threats related to the access control system, it is possible to formulate a threat model of the access control system, where the actions of the intruder will be described. As a violator, whose actions are aimed at unauthorized access to information processed in computer systems, a subject should be considered who has access to work with standard means of information systems.

The following levels of the intruder's functionality are distinguished, having a hierarchical relationship, according to which the higher level includes the functionality of the previous one:

- creation and launch of profiles with new capabilities for information processing;
- management of the operation of access control systems, impact on the basic settings, composition and configuration of access control systems equipment.

With regard to computer systems, it is natural to believe that violators of the first two categories are likely to violate information security, and a software attack is the highest form of security threat.

Today, in the construction of an access control system, the final word belongs to the system administrator for the protection of information in computer systems. It is he who sets up the elements of the access control system. These elements include database protection tools, technologies for building local and global computing systems, technologies for building telecommunications systems, technologies and information security tools, etc.

We will build a threat model from the development of an informal attack model. To implement an attack, an attacker simulates some security event, which subsequently leads to the desired result. The first two stages of the informal model are applied to implement a security event, i.e. some action in relation to the addressee to achieve a result that leads to a violation of the security policy. By vulnerability we mean a characteristic of an access control system, the use of which by an intruder can lead to the implementation of a threat. An informal attack model can be represented as follows (Figure 1). Always when assessing a threat, it is necessary to determine the likelihood of its implementation, and when it manifests itself, what harm it can bring.

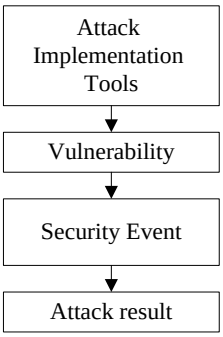

Fig. 1. Informal model of software attack

From an informal model, one can move to a threat model. It is most rational to build a threat model according to the block principle, where each block corresponds to the *i*-th threat state. This threat model is

shown in Figure 2. The model covers the following states:

S_0 - state, initial or safe state of the access control system;

S_1 - a condition leading to an unauthorized user to authenticate himself;

S_2 - state, unauthorized modification or copying of data;

S_3 - status, cracking a password or other means of passing authentication;

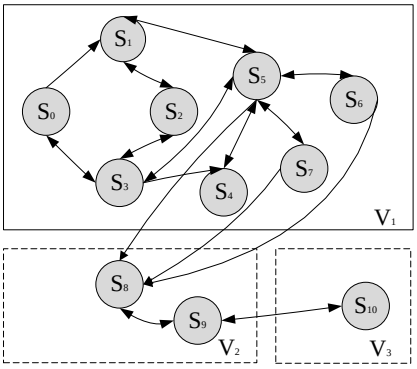

Fig 2. Security threat state model

S_4- state, data theft;

S_5- state, unauthorized obtaining of authority to work in the COP;

S_6 - state, unauthorized creation of a new illegal user;

S_7- state, unauthorized introduction of malicious programs and codes;

S_8- state, unauthorized termination of the computer network;

S_9- state corresponding to access support;

S_{10} - the state corresponding to the concealment of the attack;

V_1 - a subset of states of preparation of an attack (destruction of confidentiality);

V_2 is a subset of states of attack implementation (establishing control over the network);

V_3 is a subset of attack completion states (destruction of integrity).

The threat system is characterized by three subsets of events: V_1, V_2, and V_3. In the first subset of events V_1, an attacker studies the network environment, identifies the network topology, identifies active network nodes, identifies services, port scans, identifies operating systems, determines the role of a network node, identifies network vulnerabilities, and prepares the attack on the network itself.

In the second subset V_2, there is direct access to the services and resources of the network and an attempt to establish control over the network.

The third subset V_3 is characterized by the stages of supporting network re-accesses and attack concealment.

The final state of the system will be precisely the state S_{10}, since the intruder will always try to leave for himself the method of re-entering the network. Such a threat implementation as "denial of service" will be considered as an extreme measure, and this threat is preceded by stages that are fully described in the presented model.

External factors affecting the model will be whether the attackers have network scanners, their professional training, awareness of the network structure and information security systems, social engineering, etc.

The probability of the state *S(t)* of the threat system at time *t* is considered as a set of unconditional probabilities of the system being in the state S_t , which are determined by the expression.

$$P_i(t) = P(S(t) = s_i) \qquad (1)$$

where, *S(t)* is the random state of the system at the moment *t, i = 1, 2, 3,..,n*.

The transition probability is defined as follows:

$$P_{ij}(t) = P\big(S(k) = s_j \big| S\ (k-1) = s_j\big) \quad (2)$$

Applying the formula of total probability and passing from the *(k-1)* -th and k-th steps, we obtain the required expression in recurrent form to determine the unconditional probabilities of finding the threat system at the *k*-th step:

$$P_j(k) = \sum_{i=1}^{n} P_i(k-1)P_{il} \qquad (3)$$

The threat state model is limited by its intended purpose, i.e. by modeling external and internal threats to the organization's computing systems. So, if the structure of the model has been defined, the algorithm for carrying out the attack has been developed, then now it is necessary to determine the parameters of the threat affecting computer systems. Since it is necessary to consider this model as an integral and most important part of the information security model, it is imperative to take into account the opposition from the security system and the nature of the confrontation of competing systems. The complexity of choosing the parameters of the threat model is determined by the behavioral uncertainty of the threat system.

The main parameters of the threat model will be the probabilities of the impact of the threat system on the information protection system of computer systems and the probability of opening the information protection system.

Let us move from the system state model shown in Figure 3 to the model presented in the form of a labeled graph, where D_i will denote the state of the security system, μ_i are the intensities aimed at restoring the information security system, γ_i is the intensity of opening the security system, P_i are the state of attacks events.

Let us introduce the following notation:

P_1- no external attack was performed;

P_2-made an external attack;

P_3-an internal type attack was performed;

P_4- an unknown type of attack was performed;

P_5- an attack was made on the control system.

Let the system states have the following designations:

D_1 - safe state of the protection system (the system is not susceptible to attacks), i.e. safe initial state of the system;

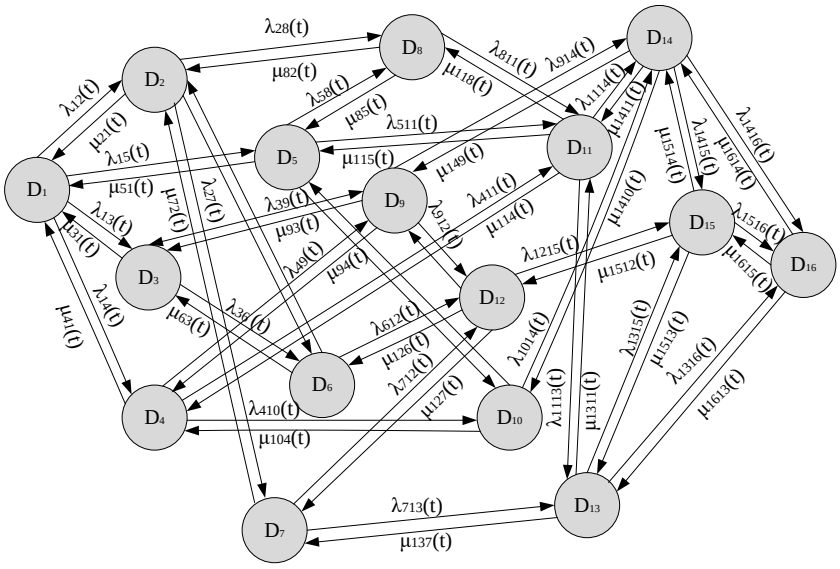

Fig. 3.The marked graph of the state of the protection system

D_2 - the state of the system in which the external attack was performed. This is the state of the system *(*S_1, S_3) of the system model;

D_3 - the state of the system when performing an external attack, This state corresponds to the state of the system S_1, S_4, S_6;

D_4 - the state of the system under which the attack was carried out through the control system. System states - S_5;

D_5 - An unknown type of attack was made. State S_{10}.

D_6 - the state of the system, with the simultaneous occurrence of states P_1, P_3 and no occurrence of states P_2, P_4, P_5.

D_7 - the state of the system, with the simultaneous occurrence of states P_2 and P_4 and the occurrence of states P_1, P_3, P_5.

D_8 - the state of the system, with the simultaneous occurrence of states P_2 and P_5 and no occurrence of states P_1, P_3, P_4.

D_9 - the state of the system, with the simultaneous occurrence of the states P_3 and P_4 and the non-occurrence of the states P_1, P_2, P_5.

D_{10} - the state of the system, with the simultaneous occurrence of the states P_3 and P_5 and the non-occurrence of the states P_1, P_2, P_4.

D_{11} - the state of the system, with the simultaneous occurrence of the states P_4 and P_5 and the non-occurrence of the states P_1, P_2, P_3.

D_{12} - the state of the system, with the simultaneous occurrence of states P_2, P_3, P_4 and the occurrence of states P_1, P_5.

D_{13} - the state of the system, with the simultaneous onset of states P_2, P_4, P_5 and the onset of state P_3.

D_{14} - the state of the system, with the simultaneous onset of states P_3, P_4, P_5 and not the onset of state P_2.

D_{15} - the state of the system, with the simultaneous onset of states P_2, P_3, P_5 and the onset of state P_4.

D_{16} - the state of the system, with the simultaneous onset of states P_2, P_3, P_4, P_5 and the onset of state P_1.

Let's introduce a number of restrictions into the model.

1) all states of the system D_1, D_2, …, D_{16} are independent events;

2) attack streams are Poisson with variable intensities $\lambda_i(t)$;

3) the protection system will respond to the threat flows with the flows of countering threats and restoring the information protection system, these intensities will be denoted by $\mu_i(t)$.

Labeled graph state protection system is shown in Fig.3.

For clarity, the flows of attacks $\lambda_i(t)$ and flows of countering attacks $\mu_i(t)$ are indicated by arrows "⇆" in the figure.

The matrix of intensities of the protection system was adjusted according to the system state graph:

$$\|\lambda_B(t)\| = \begin{vmatrix} 0 & \lambda_{12} & \lambda_{13} & \lambda_{14} & \lambda_{15} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_{21} & 0 & 0 & 0 & 0 & \lambda_{26} & \lambda_{27} & \lambda_{28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_{31} & 0 & 0 & 0 & 0 & \lambda_{36} & 0 & 0 & \lambda_{39} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_{41} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{49} & \lambda_{410} & \lambda_{411} & 0 & 0 & 0 & 0 & 0 \\ \mu_{51} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{58} & 0 & \lambda_{510} & \lambda_{511} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu_{62} & \mu_{63} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{612} & 0 & 0 & 0 & 0 \\ 0 & \mu_{72} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{712} & \lambda_{713} & 0 & 0 & 0 \\ 0 & \mu_{82} & 0 & 0 & \mu_{85} & 0 & 0 & 0 & 0 & 0 & \mu_{811} & 0 & 0 & \lambda_{914} & 0 & 0 \\ 0 & 0 & \mu_{93} & \mu_{94} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{912} & 0 & \lambda_{1014} & 0 & 0 \\ 0 & 0 & 0 & \mu_{104} & \mu_{105} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1114} & \lambda_{1215} & \lambda_{1216} \\ 0 & 0 & 0 & \mu_{114} & \mu_{115} & 0 & 0 & \mu_{118} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{1315} & \lambda_{1316} \\ 0 & 0 & 0 & 0 & 0 & \mu_{126} & \mu_{127} & 0 & \mu_{129} & 0 & 0 & 0 & 0 & 0 & \lambda_{1415} & \lambda_{1416} \\ 0 & 0 & 0 & 0 & 0 & 0 & \mu_{137} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{149} & \mu_{1410} & \mu_{1411} & 0 & 0 & 0 & \lambda_{1415} & \lambda_{1416} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{1512} & \lambda_{1513} & \lambda_{1514} & 0 & \lambda_{1516} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mu_{1612} & \mu_{1613} & \mu_{1614} & \mu_{1615} & 0 \end{vmatrix}$$

Knowing the marked graph or the intensity matrix, you can use the mnemonic rule and write down a system of differential equations for the probabilities of the state of the information security system.

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\lambda_{ij}(t) - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t) \quad (4)$$

Based on (4), we obtain the following system of equations:

$$\begin{cases} p_1 = p_2\mu_{21} + p_3\mu_{31} + p_4\mu_{41} + p_5\mu_{51} - p_1(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15}) \\ p_2 = p_1\lambda_{12} + p_6\mu_{62} + p_7\mu_{72} + p_8\mu_{82} - p_2(\mu_{21} + \lambda_{26} + \lambda_{27} + \lambda_{28}) \\ p_3 = p_1\lambda_{13} + p_6\mu_{63} + p_9\mu_{93} - \rho_3(\mu_{31} + \lambda_{36} + \lambda_{39}) \\ p_4 = p_1\lambda_{14} + p_9\mu_{94} + p_{10}\mu_{104} + p_{11}\mu_{114} - p_4(\mu_{41} + \lambda_{49} + \lambda_{410} + \lambda_{411}) \\ p_5 = p_1\lambda_{15} + p_8\mu_{85} + p_{10}\mu_{105} + p_{11}\mu_{115} - p_5(\mu_{51} + \lambda_{58} + \lambda_{510} + \lambda_{511}) \\ p_6 = p_2\lambda_{26} + p_3\lambda_{36} + p_{12}\mu_{126} - p_6(\mu_{62} + \mu_{63} + \lambda_{612}) \\ p_7 = p_2\lambda_{27} + p_{12}\mu_{127} + p_{13}\mu_{137} - p_7(\mu_{72} + \lambda_{712} + \lambda_{713}) \\ p_8 = p_2\lambda_{28} + p_5\lambda_{58} + p_{11}\mu_{118} - p_8(\mu_{82} + \mu_{85} + \lambda_{812}) \\ p_9 = p_3\lambda_{39} + p_4\lambda_{49} + p_{12}\mu_{129} + p_{14}\mu_{149} - p_9(\mu_{93} + \mu_{94} + \lambda_{912} + \lambda_{914}) \\ p_{10} = p_4\lambda_{410} + p_5\lambda_{510} + p_{14}\lambda_{1410} - p_{10}(\mu_{104} + \mu_{105} + \lambda_{1014}) \\ p_{11} = p_4\lambda_{411} + p_5\lambda_{511} + p_8\lambda_{811} + p_{14}\mu_{1411} - p_{11}(\mu_{114} + \mu_{115} + \lambda_{1114}) \\ p_{12} = p_6\lambda_{612} + p_7\lambda_{712} + p_9\lambda_{912} + p_{15}\mu_{1512} + p_{16}\mu_{1612} - p_{12}(\mu_{1216} + \mu_{1217} + \mu_{129} + \lambda_{1215} + \lambda_{1216}) \\ p_{13} = p_7\lambda_{713} + p_{15}\mu_{1513} + p_{16}\mu_{1613} - p_{13}(\mu_{137} + \lambda_{1315} + \lambda_{1316}) \\ p_{14} = p_9\lambda_{914} + p_{10}\lambda_{1014} + p_{11}\lambda_{1114} + p_{15}\mu_{1514} + p_{16}\mu_{1614} - p_{14}(\mu_{1419} + \mu_{1410} + \mu_{1411} + \lambda_{1415} + \lambda_{1416}) \\ p_{15} = p_{12}\lambda_{1215} + p_{13}\lambda_{1315} + p_{14}\lambda_{1415} + p_{16}\mu_{1615} - p_{15}(\mu_{1512} + \mu_{1513} + \mu_{1514} + \lambda_{1516}) \\ p_{16} = p_{12}\lambda_{1216} + p_{13}\lambda_{1316} + p_{14}\lambda_{1416} + p_{15}\mu_{1516} - p_{16}(\mu_{1612} + \mu_{1613} + \mu_{1614} + \lambda_{1615}) \end{cases}$$

In this system of equations $p_i = p_i(t), \lambda_y = \lambda_y(t), \mu_y = \mu_y(t)$

This system of differential equations will be solved under the initial conditions that specify the probabilities of states at the initial moment of time at $t = 0$ $P_1(0), P_2(0), \dots\dots\dots P_{16}(0)$. Moreover, we will take into account that for any moment of time *t* the normalized condition is satisfied, $P_1+P_2+P_3+P_4+P_5+P_6+P_7+P_8+P_9+P_{10}+P_{11}+P_{12}+P_{13}+P_{14}+P_{15}+P_{16}=1$.

For this model, we make the following first assumption.

Today, there are network attacks designed to disable a computing system. One request immediately destroys the computing system. Based on the above, let us assume that all flow rates $\mu_{ij}(t)\lambda_{ij}(t)$ are independent of the argument *t*. Then we get a homogeneous Markov process. Consequently, all the coefficients in the resulting system of differential equations are constant numbers, this will greatly facilitate the solution of these equations. According to the assumptions made, we set the initial condition for solving the differential equation

$$P_1(0) = 1, P_i(0) = 0, I = 1,2,3, \dots\dots\dots 16.$$

This means that at the initial moment of time there were no attacks on the system, i.e. the system was in a safe state D_1.

When solving a system of differential equations, any of the equations can be discarded, and the corresponding probability $P_1(t) = 1$, $I = 1,2,3, \dots\dots\dots 16$ can be expressed in terms of all the others using the normalized condition. This system of

differential equations can be solved by any of the numerical methods.

The second assumption will be $\mu_{ij} = \text{const}$ and $\lambda_{ij} = \text{const}$.

Then, instead of a system of homogeneous differential equations with constant coefficients for the probabilities of the state of the system, we obtain a system of homogeneous algebraic equations with constant coefficients for images of the probabilities of states. This system can be solved taking into account the standardized condition

$$\sum_{i=1}^{16} p_1(t) = 1, (0 \le p_1(t) \le 1; t \ge 0)$$

$$x\pi_i(x) = \sum_{j=1}^{m} \lambda_{ij}\pi_i(x) + p_i(0), \textit{(i=1,2, ..., n} \quad (5)$$

From equation (5) we obtain:

$$x\pi_1(x) = \mu_{21}\pi_2(x) + \mu_{31}\pi_3(x) + \mu_{41}\pi_4(x)+\mu_{51}\pi_5(x) - \pi_1(x)(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15}) + 1$$
$$x\pi_2(x) = \lambda_{12}\pi_1(x) + \mu_{62}\pi_6(x) + \mu_{72}\pi_7(x)+\mu_{82}\pi_8(x) - \pi_2(x)\left(\mu_{21} + \lambda_{26} + \lambda_{27} + \lambda_{28}\right)$$
$$x\pi_3(x) = \lambda_{13}\pi_1(x) + \mu_{63}\pi_6(x) + \mu_{93}\pi_9(x) - \pi_3(x)\left(\mu_{31} + \lambda_{36} + \lambda_{39}\right)$$
$$x\pi_4(x) = \lambda_{14}\pi_1(x) + \mu_{94}\pi_9(x) + \mu_{164}\pi_{10}(x)+\mu_{114}\pi_{11}(x) - \pi_4(x)\left(\mu_{41} + \lambda_{49} + \lambda_{410} + \lambda_{411}\right)$$
$$x\pi_5(x) = \lambda_{15}\pi_1(x) + \mu_{85}\pi_8(x) + \mu_{105}\pi_{10}(x)+\mu_{115}\pi_{11}(x) - \pi_5(x)\left(\mu_{51} + \lambda_{58} + \lambda_{510} + \lambda_{511}\right)$$
$$x\pi_6(x) = \lambda_{26}\pi_2(x) + \lambda_{36}\pi_3(x) + \mu_{126}\pi_{12}(x) - \pi_6(x)\left(\mu_{62} + \mu_{63} + \lambda_{612}\right)$$
$$x\pi_7(x) = \lambda_{27}\pi_2(x) + \mu_{127}\pi_{12}(x)+\mu_{137}\pi_{13}(x) - \pi_7(x)\left(\mu_{72} + \mu_{74} + \lambda_{712} + \lambda_{713}\right)$$
$$x\pi_8(x) = \lambda_{28}\pi_2(x) + \lambda_{58}\pi_5(x) + \mu_{118}\pi_{11}(x) - \pi_8(x)\left(\mu_{82} + \mu_{85} + \lambda_{812}\right)$$
$$x\pi_9(x) = \lambda_{39}\pi_3(x) + \lambda_{49}\pi_4(x) + \mu_{129}\pi_{12}(x)+\mu_{149}\pi_{14}(x) - \pi_9(x)\left(\mu_{93} + \mu_{94} + \lambda_{912} + \lambda_{914}\right)$$
$$x\pi_{10}(x) = \lambda_{410}\pi_4(x) + \lambda_{510}\pi_5(x) + \lambda_{1410}\pi_{14}(x) - \pi_{10}(x)\left(\mu_{104} + \mu_{105} + \lambda_{1014}\right)$$
$$x\pi_{11}(x) = \lambda_{411}\pi_4(x) + \lambda_{511}\pi_5(x) + \lambda_{811}\pi_8(x)+\mu_{1411}\pi_{14}(x) - \pi_{11}(x)\left(\mu_{114} + \mu_{115} + \lambda_{1114}\right)$$
$$x\pi_{12}(x) = \lambda_{612}\pi_6(x) + \lambda_{712}\pi_7(x) + \lambda_{912}\pi_9(x)+\mu_{1512}\pi_{15}(x) + \mu_{1612}\pi_{16}(x) - \pi_{12}(x)\left(\mu_{1216} + \mu_{1217} + \mu_{129} + \lambda_{1215} + \lambda_{1216}\right)$$
$$x\pi_{13}(x) = \lambda_{713}\pi_7(x) + \mu_{1513}\pi_{15}(x) + \mu_{1613}\pi_{16}(x)+\mu_{1613}\pi_{16}(x) - \pi_{13}(x)\left(\mu_{137} + \lambda_{1315} + \lambda_{1316}\right)$$
$$x\pi_{14}(x) = \lambda_{914}\pi_9(x) + \lambda_{1014}\pi_{10}(x) + \lambda_{1114}\pi_{11}(x)+\mu_{1514}\pi_{15}(x)+\mu_{1614}\pi_{16}(x) - \pi_{14}(x)\left(\mu_{1419} + \mu_{1410} + \mu_{1411} + \lambda_{1415} + \lambda_{1416}\right)$$
$$x\pi_{15}(x) = \lambda_{1215}\pi_{12}(x) + \lambda_{1315}\pi_{13}(x) + \lambda_{1415}\pi_{14}(x) + \mu_{1615}\pi_{16}(x) - \pi_{15}(x)\left(\mu_{1512} + \mu_{1513} + \lambda_{1514} + \lambda_{1516}\right)$$
$$x\pi_{16}(x) = \lambda_{1216}\pi_{12}(x) + \lambda_{1316}\pi_{13}(x) + \lambda_{1416}\pi_{14}(x) + \mu_{1516}\pi_{16}(x) - \pi_{16}(x)\left(\mu_{1612} + \mu_{1613} + \lambda_{1614} + \lambda_{1615}\right)$$
$$\pi_1(x) + \pi_2(x) + \pi_3(x) + \pi_4(x) + \pi_5(x) - \pi_6(x) + \pi_7(x) + \pi_8(x) + \pi_{10}(x) + \pi_{11}(x) + \pi_{12}(x) + \pi_{13}(x) + \pi_{14}(x) + \pi_{15}(x) + \pi_{16}(x) = \frac{1}{x}$$

The resulting system of equations can be simplified. We will assume that the process proceeding in the system with a certain probability takes place near any other state. Let all streams of events transferring the system from state to state be the simplest ones with constant intensities. Consequently, for a stationary mode of operation, the system of Kolmogorov differential equations is transformed into a system of homogeneous algebraic equations with constant coefficients:

$$o = \sum_{j=1}^{n} \lambda_{ij} p_i - p_i \sum_{j=1}^{n} \lambda_{ij} \quad (8)$$

$$\pi_i(x) = \frac{\sum_{j=1}^{n} \lambda_{ij}\pi_j(x)+p_i(0)}{x+\lambda_i} = \frac{\sum_{j=1}^{n} \lambda_{ij}\pi_j(x)+p_i(0)}{x+\sum_{j=1}^{n} \lambda_{ij}} \quad (6)$$

Consequently, one of the equations of the resulting system and images of the probabilities $p_i(t)$ can be replaced with a simpler expression.

$$\sum_{j=1}^{n} \pi_i(x) = \frac{1}{x} \quad (7)$$

Expression (7) is an image of the normal condition:

Expression (8) can be written as

$$p_i \sum_{j=1}^{n} \lambda_{ij} = \sum_{j=1}^{n} \lambda_{ij} p_i \quad (9)$$

Equation (9) can be reduced to a simpler form:

$$p_i = \frac{\sum_{j=1}^{n} \lambda_{ij} p_i}{\lambda_i} \quad (i = 1,2,3, \dots, n), \text{где } \lambda_i = \sum_{j=1}^{n} \lambda_{ij}$$

To solve a system of algebraic equations, one of these equations must be replaced by the normalization condition:

$$\sum_{j=1}^{n} p_i = 1$$

Taking into account the normalization condition, we obtain the following system of algebraic equations:

$$p_1 = \frac{(\mu_{21}p_2+\mu_{31}p_3+\mu_{41}p_4+\mu_{51}p_5)}{(\lambda_{12}+\lambda_{13}+\lambda_{14}+\lambda_{15})}$$

$$p_2 = \frac{(\lambda_{12}p_1+\mu_{62}p_6+\mu_{72}p_7+\mu_{82}p_8)}{(\mu_{21}+\lambda_{26}+\lambda_{27}+\lambda_{28})}$$

$$p_3 = \frac{(\lambda_{13}p_1+\mu_{63}p_6+\mu_{93}p_9)}{(\mu_{31}+\lambda_{36}+\lambda_{39})}$$

$$p_4 = \frac{(\lambda_{14}p_1+\mu_{94}p_9+\mu_{104}p_{10}+\mu_{114}p_{11})}{(\mu_{41}+\lambda_{49}+\lambda_{410}+\lambda_{411})}$$

$$p_5 = \frac{(\lambda_{15}p_1+\mu_{85}p_8+\mu_{105}p_{10}+\mu_{115}p_{11})}{(\mu_{51}+\lambda_{58}+\lambda_{510}+\lambda_{511})}$$

$$p_6 = \frac{(\lambda_{26}p_2+\lambda_{36}p_3+\mu_{126}p_{12})}{(\mu_{62}+\mu_{63}+\lambda_{612})}$$

$$p_7 = \frac{(\lambda_{27}p_2+\mu_{127}p_{12}+\mu_{137}p_{13})}{(\mu_{72}+\lambda_{712}+\lambda_{713})}$$

$$p_8 = \frac{(\lambda_{28}p_2+\lambda_{58}p_5+\mu_{118}p_{11})}{(\mu_{82}+\mu_{85}+\lambda_{812})}$$

$$p_9 = \frac{(\lambda_{39}p_3+\lambda_{49}p_4+\mu_{129}p_{12}+\mu_{149}p_{14})}{(\mu_{93}+\mu_{94}+\lambda_{912}+\lambda_{914})}$$

$$p_{10} = \frac{(\lambda_{410}p_4+\lambda_{510}p_5+\lambda_{1410}p_{14})}{(\mu_{104}+\mu_{105}+\lambda_{1014})}$$

$$p_{11} = \frac{(\lambda_{411}p_4+\lambda_{511}p_5+\lambda_{811}p_8+\mu_{1411}p_{14})}{(\mu_{114}+\mu_{115}+\lambda_{1114})}$$

$$p_{12} = \frac{(\lambda_{612}p_6+\lambda_{712}p_7+\lambda_{912}p_9+\mu_{1512}p_{15}+\mu_{1612}p_{16})}{(\mu_{1216}+\mu_{1217}+\mu_{129}+\lambda_{1215}+\lambda_{1216})}$$

$$p_{13} = \frac{(\lambda_{713}p_7+\mu_{1513}p_{15}+\mu_{1613}p_{16})}{(\mu_{137}+\lambda_{1315}+\lambda_{1316})}$$

$$p_{14} = \frac{(\lambda_{914}p_9+\lambda_{1014}p_{10}+\lambda_{1114}p_{11}+\mu_{1514}p_{15}+\mu_{1614}p_{16})}{(\mu_{1419}+\mu_{1410}+\mu_{1411}+\lambda_{1415}+\lambda_{1416})}$$

$$p_{15} = \frac{(\lambda_{1215}p_{12}+\lambda_{1315}p_{13}+\lambda_{1415}p_{14}+\mu_{1615}p_{16})}{(\mu_{1512}+\mu_{1513}+\mu_{1514}+\lambda_{1516})}$$

$$p_{16} = \frac{(\lambda_{1216}p_{12} + \lambda_{1316}p_{13} + \lambda_{1416}p_{14} + \mu_{1516}p_{15})}{(\mu_{612} + \mu_{1613} + \mu_{1614} + \lambda_{1615})}$$

$$p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7 + p_8 + p_9 +$$

$$p_{10} + p_{11} + p_{12} + p_{13} + p_{14} + p_{15} + p_{16} = 1$$

Let us calculate the probabilities of transitions of the protection system for different intensities of attacks on the protection system and intensities of the protection system aimed at countering attacks.

The sum of λ and attack counteraction flows μ will be equal to 1. In this case λ and μ are proportional and opposite to each other.

For $\lambda = 0{,}5. P_1 - P_{16} = 0{,}0625.$

For $\lambda = 0{,}25. \mu = 0{,}75.$ $P_1 = 0{,}3116;$ $P_2, P_3, P_4, P_5 = 0{,}105;$ $P_6, P_7, P_8, P_9, P_{10}, P_{11} = 0{,}035;$ $P_{12}, P_{13}, P_{14}, P_{15} = 0{,}011;$ $P_{16} = 0{,}004.$

For $\lambda = 0{,}75. \mu = 0{,}25.$ $P_1 = 0{,}004;$ $P_2, P_3, P_4, P_5 = 0{,}012;$ $P_6, P_7, P_8, P_9, P_{10}, P_{11} = 0{,}035;$ $P_{12}, P_{13}, P_{14}, P_{15} = 0{,}105;$ $P_{16} = 0{,}316$.

For $\lambda = 1.$ $\mu = 0. P_1 - P_{15} = 0;$ $P_{16} = 1.$

For $\lambda = 1.$ $\mu = 1. P_1 = 1;$ $P_2 - P_{16} = 0.$

Based on the calculated data, let us construct a graph of the dependence of the probabilities of transitions of the protection system from one state to another on the intensity of the impact on it of threats λ and the intensity of counteraction by the protection system to these threats μ (Fig. 4).

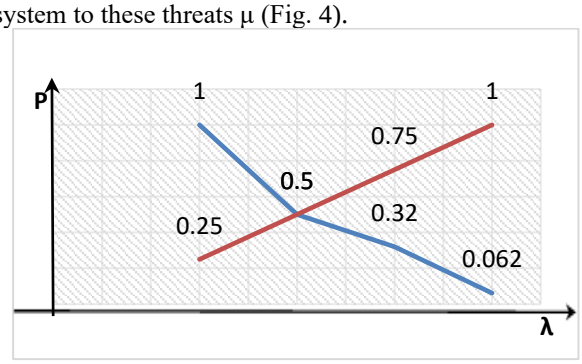

Fig.5. Dependences of the probabilities of transitions of the protection system from one state to another, depending on the impact λ and μ.

Based on the developed model, the following conclusions can be drawn:

- with the maximum impact on the protection system of attack flows and the absence of any counteraction to these attacks from the side of this system, the probability of its opening is 1;
- with equal flows of attacks and countering attacks, the probability of a complete opening of the protection system is 0.0625;
- if the information protection system is influenced by attack streams A = 0.75 and counterattack streams counter them 0.25, the probability of a complete opening of the protection system will be 0.3.

Conclusion

To effectively counteract the flows of attacks λ affecting the information security system, a countermeasures system is needed that operates with the intensity of countermeasures μ = *0.3-0.5*. Greater intensity will only increase the cost of the protection system.

To counteract the flow of attacks with such an intensity, the information protection system needs an effective system for managing the elements of protection, which functions not only at the stage of the attack, but also at the reconnaissance stage. For the implementation of timely classification and identification of threats, it is advisable to use neural network methods.

References

[1] Samarati, P.; de Vimercati, S.C. Access control: Policies, models, and mechanisms. *In Proceedings of the International School on Foundations of Security Analysis and Design, Bertinoro, Italy,* 18–30 September 2000; pp. 137–196.

[2] Cheminod, M.; Durante, L.; Seno, L.; Valenza, F.; Valenzano, A. A comprehensive approach to the automatic refinement and verification of access control policies. *Comput. Secur.* 2018. [CrossRef]

[3] Verma, D.C. Simplifying network administration using policy-based management. *IEEE Netw*. 2002, 16, 20–26. [CrossRef]

[4] Sandhu, R.; Munawer, Q. How to do discretionary access control using roles. *In Proceedings of the Third ACM Workshop on Role-Based Access Control, Fairfax, VA, USA,* 22–23 October 1998; pp. 47–54.

[5] Li, N. Discretionary access control. *In Encyclopedia of Cryptography and Security; Springer: Berlin, Germany*, 2011; pp. 353–356.

[6] Jueneman, R.R. Integrity controls for military and commercial applications. *In Proceedings of the Fourth Aerospace Computer Security Applications, Orlando, FL, USA,* 12–16 September 1988; pp. 298–322.

[7] Barabanov A.V., Dorofeev A.V., Markov A.S., Sirlov V.L. Sem bezopasnix informatsionnix texnologiy/*M.:DMK Press*, 2017- s 224. 158-160 s.

[8] Gaydamakin H.A. Razgranichenie dostupa k informatsii v kompyuternix sistemax. Izd-vo Uralskogo un-ta, 2003.- s.328.

[9] Gujva D.Yu. Teoriya i praktika neyrosetevogo upravleniya zashitoy informatsii v infotelekommunikatsionnix sistemax. *Monografiya-M: Izdatelstvo VA RVSN im. Petra Velikogo,* 2008.- 239 s.

[10] Zhu, Y.; Huang, D.; Hu, C.-J.; Wang, X. From RBAC to ABAC: Constructing flexible data access control for cloud storage services. *IEEE Trans. Serv. Comput.* 2015, 8, 601–616. [CrossRef]

[11] Batra, G.; Atluri, V.; Vaidya, J.; Sural, S. Enabling the Deployment of ABAC Policies in RBAC Systems. *In Proceedings of the 32nd IFIP Annual Conference on Data and Applications Security and Privacy, Bergamo, Italy*, 16–18 July 2018; pp. 51–68.

[12] Alam, M.; Emmanuel, N.; Khan, T.; Xiang, Y.; Hassan, H. Garbled role-based access control in the cloud. *J. Ambient Intell. Humaniz. Comput.* 2018, 9, 1153–1166. [CrossRef]

[13] Alguliev R.M., Ragimov E.R. Ob odnom metode otsenki informatsionnoy bezopasnosti korporativnix setey v stadii ix proektirovaniya//*Informatsionnыe texnologii*. 2005 - №7.

[14] Irgasheva D.Y., Rustamova, S.R. Development of Role Model for Computer System Security //*International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT* 2019, 2019, 9012058.

[15] Barkley, J. Comparing simple role based access control models and access control lists. *In Proceedings of the second ACM workshop on Role-Based Access Control, Fairfax, VA, USA,* 6–7 November 1997; pp. 127–132.

[16] Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Role-based access control models. *Computer 1996,* 29, 38–47. [CrossRef]

[17] Incits, A. Incits 359-2004. Role-based access control. *Am. Natl. Stand. Inf. Technol* 2004, 359, 2–10.

[18] Devyanin, P. N. Analiz bezopasnosti upravleniya dostupom i informatsionnimi potokami v kompyuternix sistemax [Tekst]:*Ucheb. posobie dlya vuzov/P. N. Devyanin. – M.: Radio i svyaz*, 2006. – 176 s.

[19] Teoreticheskie osnovi kompyuternoy bezopasnosti [Tekst]: *Ucheb. posobie dlya vuzov/P. N. Devyanin, O. O. Mixalskiy, D. I. Pravikov, A. Yu. Sherbakov.– M.:Radio i svyaz,* 2000. – 192 s.

[20] Ganiev, S.K., Irgasheva D.Y. About of One Methods Synthesis the Structural Protected Computer Network//*International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT* 2019, 2019, 9011891.