Advances in Military Technology
Vol. 19, No. 1, 2024, pp. 129-144
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01830

Time Aspect of Insider Threat Mitigation

V. Savchenko[1*], V. Savchenko[1], T. Dzyuba[1], O. Matsko[2], I. Novikova[2], I. Havryliuk[2], and V. Polovenko[2]

[1] *Cybersecurity Department, State University of Information and Communication Technologies, Kyiv, Ukraine*
[2] *Institute of Logistics and Troops (Forces) Support, The National Defence University of Ukraine, Kyiv, Ukraine*

The manuscript was received on 6 July 2023 and was accepted after revision for publication as research paper on 13 May 2024.

Abstract:

The article reveals the problem of mitigating an insider threat by creating a time-balanced security system in an organization. Based on Markov chain, the authors propose a basic model of interaction in an "organization – insider" system. The article analytically defines a ratio between the time of an insider attack and the time during which the organization's security system can neutralize it. The authors propose a concept of a multi-level system of organization protection, which takes into account the involved resources and practical skills of employees, as well as security services. At the end of the article, it is concluded that the proposed concept of the organization's protection system will be effective against potential insider attacks.

Keywords:

cyber attack, security system, insider threat, Markov chain, time balance

1 Introduction

Day by day, information security is becoming increasingly important. Companies make significant investments to protect their computer networks from hackers and viruses, as well as to protect individual computers and premises from unauthorized remote retrieval of information, and transmitted information from decryption. Increasing the amount of stored electronic information and the number of employees in the organization who have access to it, increase opportunities for information theft or distortion in favor of competitors, which makes the problem of mitigating insider threats urgent [1].

[*] *Corresponding author: Cybersecurity Department, State University of Information and Communication Technologies, Solomianska str. 7, Kyiv, UA-03110 Ukraine. Phone: +380 442 49 25 35, +380 675 04 60 12, E-mail: savitan@ukr.net. ORCID 0000-0002-3014-131X.*

Understanding the insider threat and how to deal with it can help shape mitigation strategies, including technical, organizational, and social tools. The peculiarity of the study of insider threat is that: 1) an insider can be any employee of the company, regardless of role, position, and time of work within the company; 2) work with the company's staff by raising suspicions does not give the desired effect; 3) organizations are extremely reluctant to share information about problems in internal security and therefore the statistics of methods of work of insiders and counteraction to them by security services are extremely limited. Therefore, the primary method of studying the problem of insider threat is modelling.

2 Statement of Research Problem

Traditionally, modelling of insider threats focuses on behavioral and psychological methods, considering the identity of the potential violator and forecasting the incidents of insider threat. Most of these models are statistical and they aim to predict employee behavior based on trends using different regression models. An extensive overview of the models was done in [2].

At the same time, behavioral models alone do not give an idea of how an effective system of protection against insider threats should be built. Existing behavioral models do not consider the dynamics of the interaction of a potential insider with the security system of the organization. In particular, it remains unclear what should be the distribution of roles of employees according to their qualifications and speed of work with information. On the one hand, the most skilled workers, who have access to the most important information and can process it quickly, must do the basic work. Here, the organization will use human resources most efficiently. However, then the defense system is left with less qualified employees who cannot do the job quickly, which can lead to a backlog of the protection system and create additional vulnerabilities from insiders.

Insider threat is a dynamic process that develops according to certain laws and therefore, it is the change of certain parameters of the system "organization – insider" over time, which is of scientific interest. It is logical to assume that reactions of the organization's defense system should be ahead of any potential insider.

3 Overview of Related Works

Markov models are one of the most common for modelling the dynamics of insider interaction with protecting the organization. Thus, publication [3] proposed building a mathematical model of countering threats in the system of protecting the organization's critical information resources using Markov chain. The authors developed a technique for identifying current threats to data security during data processing. Such an approach makes it possible to determine and model the parameters of various types of attacks, including insiders', with an emphasis on the probability of saving information without taking into account the time parameters of protection.

Publication [4] provides a method for detecting insider attacks by detecting anomalies based on the Markov chain model, which represents the transition profile of computer events in the network system. The more the observed user activity differs from the normal model of the Markov chain, the greater the probability of an anomaly because of an insider attack. The article also notes that Markov circuit technology is not completely reliable in terms of data noise (the level of combination of normal and

anomalous activity), and the desired performance can be achieved only at low noise levels.

In the article [5], the optimization problem for the choice of means of information protection using Markov's cyber threat model is formulated and the possibility of solving the problem by the method of sequential analysis of variants is analyzed. The article provides a clear analytical formula for the average service life of the information system, expressed in terms of the initial parameters of the model, which are the probabilities of the threat and the probability of its elimination by security.

The publication [6] is devoted to the quantitative assessment of security risk by modelling dependencies when a sequence of dangerous actions of attackers or personnel is performed to launch a successful cyberattack. To estimate the probability of security risk for systems that suffer from successive cyberattacks, Continuous-time Markov chains and methods based on semi-Markov processes are proposed. Although the Continuous-time Markov Chain (CTMC) method is limited by the exponential state transition time, the proposed approach, based on a semi-Markov process, is used to analyze attacks with any arbitrary type of transition time distribution.

Calculating the probability of an attack, or rather the threat that materializes in an attack, is an important basis for quantitative security metrics. Authors of [7] consider an approach to calculating the distribution of probabilities of security threats based on the Markov chain with the calculation of the overall vulnerability.

Publication [8] considers stochastic modelling of cyber threats acting on computer systems based on the Markov chain. Here, computer systems are considered as systems with failures and recoveries by analogy with the models of technical systems in the theory of reliability. Considering cyber threats as independent random events, explicit analytical formulas are obtained for the probabilities of the state of the corresponding Markov chain and the Mean Time to Security Failure (MTSF). With dependent cyber threats, it is possible to obtain approximate expressions for state probabilities and MTSF in the framework of first-order perturbation theory. With this approach, the average reaction time is one of the determining factors, although such a model is extremely generalized and cannot be used to find a rational ratio between the elements of the security system.

The current work does not claim to be complete but it suggests that for a long time, there is the idea of creating a comprehensive model of the insider, which is currently not implemented because of the significant difficulties of separating insider behavior from the behavior of honest users. Another problem in creating an effective insider model is its separation from the organization's security system. In our opinion, an insider who is part of an organization should be considered as an integral part of it and in the system "organization – insider" in order to determine certain types of activities of the attacker appropriate countermeasures.

Modeling of the "organization – insider" system can be carried out in various aspects. The aspect of interaction time in such a system remains understudied because, despite the obvious fact that the defense must be more agile than the attack, the problem of the ratio of the reaction time of the defense to the time of the attack has not yet been studied.

The purpose of the article is to study the time factor of insider threat mitigation and to determine the main time parameters of the organization's system of protection against insider threats.

4 Basic Model of Insider Threat

Practical attempts to develop a detailed model of cyberattacks have been made before. Today, the best known models are Lockheed Martin Cyber Kill Chain [9] and MITRE ATT&CK frameworks [10], which describe in detail the steps and technologies of attacks. However, these approaches cover mainly external attacks, which have a significant number of features compared to internal threats. In [11, 12] authors propose an adapted model as well as a matrix of actions for internal attack.

For further research on the basis of [11], we will create a typical model in the form of a Markov chain with discrete states and continuous time (Fig. 1).

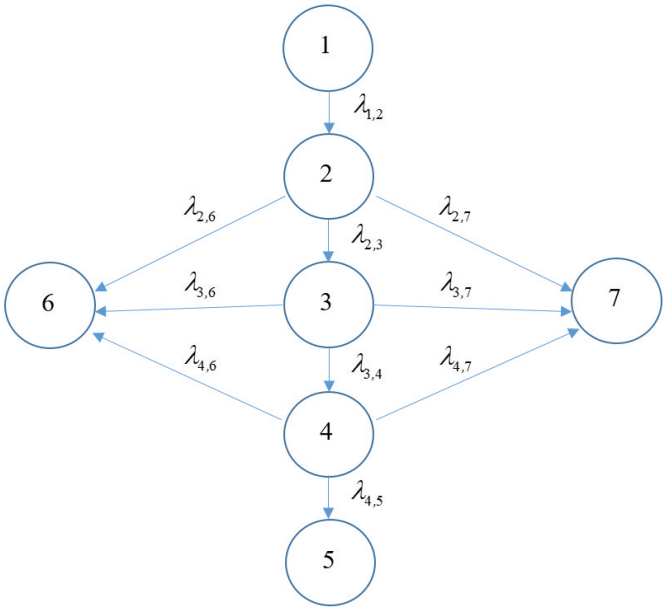

Fig. 1 Markov model of insider threat

This model describes the activities of a potential insider in the form of a sequence of states 1, 2, 3, 4, 5, after which he can succeed (state 5): 1 – normal work of the employee in the organization; 2 – risk analysis, preparation for the attack; 3 – attack (login, data search, verification, data copying or weaponize); 4 – destruction of traces of attack or impact; 5 – use of the extracted information.

Transitions from one state to another are determined only by the ability of a potential insider to perform certain actions in the system and they almost do not depend on the activities of security services. Upon closer examination, it can also be assumed that the employee's intention to become an insider will also be determined by his own predictions of further consequences, which depend on the organization's ability to resist such attempts. However, at this stage these aspects are not considered. Chain of transitions $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5$ describes the activities of an insider to achieve his desired goal – to obtain and use information from the organization or influence such information.

The model also provides two more states that directly characterize the capabilities of the protection system: 6 – interception of the attack by the security service; 7 – refusal of the insider from carrying out attack.

We will assume that these conditions depend solely on the characteristics of the protection service (state 6) and technical means of monitoring the activities of employees of the organization (state 7). Transitions $6 \leftarrow 2 \rightarrow 7$, $6 \leftarrow 3 \rightarrow 7$ and $6 \leftarrow 4 \rightarrow 7$ form three boundaries of protection in the organization and depend only on the capabilities of the security system.

Thus, going from state 1 to state 2, the insider has two options: either to go further to state 3, while implementing his own attack plan, or to be intercepted by the security system, getting to state 6, or to abandon further intentions, moving to state 7.

An important element for further consideration is the intensity indicators, $\lambda_{i,j}$, $i, j = 1,\ldots,7$ which describe the dynamics of the system. The intensity of transitions is an inverse characteristic of the average time spent on the transition to a certain state from the previous one

$$\lambda_{i,j} = \frac{1}{\overline{t}_{i,j}} \quad i, j = 1,...,7 \tag{1}$$

The behavior of the system can be described using Kolmogorov differential equations:

$$\begin{aligned}
\frac{\mathrm{d}P_1(t)}{\mathrm{d}t} &= -\lambda_{1,2}P_1(t) \\
\frac{\mathrm{d}P_2(t)}{\mathrm{d}t} &= \lambda_{1,2}P_1(t) - \lambda_{2,3}P_2(t) - \lambda_{2,6}P_2(t) - \lambda_{2,7}P_2(t) \\
\frac{\mathrm{d}P_3(t)}{\mathrm{d}t} &= \lambda_{2,3}P_2(t) - \lambda_{3,4}P_3(t) - \lambda_{3,6}P_3(t) - \lambda_{3,7}P_3(t) \\
\frac{\mathrm{d}P_4(t)}{\mathrm{d}t} &= \lambda_{3,4}P_3(t) - \lambda_{4,5}P_4(t) - \lambda_{4,6}P_4(t) - \lambda_{4,7}P_4(t) \\
\frac{\mathrm{d}P_5(t)}{\mathrm{d}t} &= \lambda_{4,5}P_4(t) \\
\frac{\mathrm{d}P_6(t)}{\mathrm{d}t} &= \lambda_{2,6}P_2(t) + \lambda_{3,6}P_3(t) + \lambda_{4,6}P_4(t) \\
\frac{\mathrm{d}P_7(t)}{\mathrm{d}t} &= \lambda_{2,7}P_2(t) + \lambda_{3,7}P_3(t) + \lambda_{4,7}P_4(t)
\end{aligned} \tag{2}$$

Assume that from the beginning, the system is in a state of normal operation (state 1) and therefore the initial conditions for differentiation at time $t = 0$ will be:

$$P_1(0) = 1;\ P_2(0) = 0;\ P_3(0) = 0;\ P_4(0) = 0;\ P_5(0) = 0;\ P_6(0) = 0;\ P_7(0) = 0 \tag{3}$$

Let us consider for example the implementation of the model for arbitrary initial conditions: $\lambda_{1,2} = \frac{1}{12}$; $\lambda_{2,3} = \frac{1}{12}$; $\lambda_{3,4} = \frac{1}{6}$; $\lambda_{4,5} = \frac{1}{3}$; $\lambda_{2,6} = \frac{1}{24}$; $\lambda_{3,6} = \frac{1}{12}$; $\lambda_{4,6} = \frac{1}{6}$; $\lambda_{2,7} = \frac{1}{30}$; $\lambda_{3,7} = \frac{1}{15}$; $\lambda_{4,7} = \frac{1}{6}$; $t_{\max} = 60$.

In this case, the implementation of the system of equations will look like this (Fig. 2). As you can see, the probability of the system being in state 1 gradually decreases (P_1). At the same time, the probability of the insider achieving his goal (P_5), the probability of interception of the insider by the security service (P_6) and the probability of the insider's refusal to further action (P_7) increase.

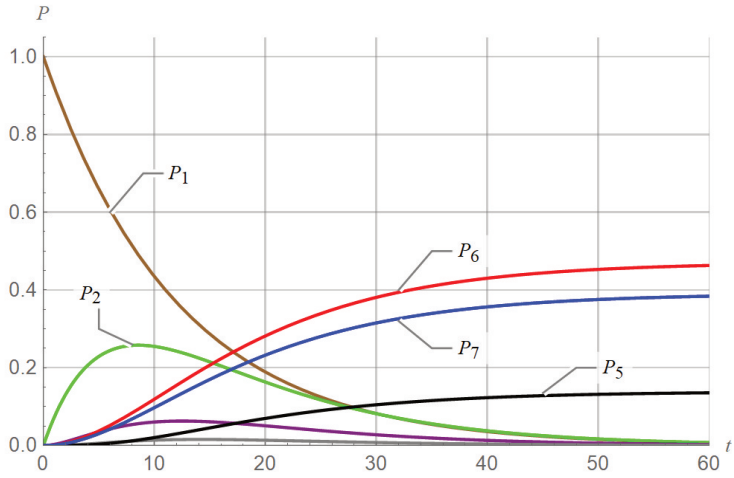

Fig. 2 Probabilities of system states: P_1 – the probability of the system being in the initial state; P_5 – the probability of a successful insider attack; P_6 – the probability that the insider will be caught; P_7 – the probability that the insider will refuse the attack. All other curves are the probabilities of states 2-5.

To build an effective protection system, it is necessary to minimize the probability of an insider achieving his goal P_5. The control parameters in the model are intensities $\lambda_{i,j}$, $i, j = 1,\ldots,7$. Thus, selecting the required ratio of intensity parameters $\lambda_{i,j}$ you can build a security system in which the probability of a successful attack by an insider will be minimal. The problem of creating an effective protection system based on time balance is as follows: Find the optimal values of the parameters $\lambda_{i,j}$, which lead to minimization of probability P_5 in the field of stationary solutions.

Solve the first equation in system (2) taking into account $p_1(0)=1$ in initial conditions (3):

$$p_1(t)=\mathrm{e}^{-\lambda_{1,2}t} \tag{4}$$

Substituting (4) into the second equation of system (2) and solving it under the condition that $p_2(0)=0$, we get the equation for P_2

$$p_2(t)=\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left[\mathrm{e}^{-\lambda_{1,2}t}-\mathrm{e}^{-\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\right] \tag{5}$$

Since the function (5) has discontinuities at the points defined by the expression $\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}=0$, it is appropriate to investigate such discontinuities. Taking the Limit of function (5) from above and below, you can see that

$$\begin{aligned}&\lim_{\lambda_{1,2}\to\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)^{+}}\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left[\mathrm{e}^{-\lambda_{1,2}t}-\mathrm{e}^{-\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\right]=\\&\lim_{\lambda_{1,2}\to\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)^{-}}\frac{\lambda_{1,2}}{\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{1,2}}\left[\mathrm{e}^{-\lambda_{1,2}t}-\mathrm{e}^{-\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\right]=\\&=\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t\mathrm{e}^{-\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}=\lambda_{1,2}t\mathrm{e}^{-\lambda_{1,2}t}\end{aligned} \tag{6}$$

Thus, it can be concluded that the specified discontinuities are "removable", which makes it possible to determine the value of (5) at the discontinuity points as $p_2(t) = \lambda_{1,2} t \mathrm{e}^{-\lambda_{1,2} t}$. Using this approach, in the future we will assume that the derived functions for $p_3(t), p_4(t), p_5(t)$ will have certain values at the discontinuity points.

Since further calculations are associated with cumbersome mathematical operations, in order not to lose symbols in formulas and to ensure the correctness of writing expressions for further calculations, we will use the system of symbolic calculations (in our case, Wolfram Mathematica). Substituting (5) into the third equation of (2) and solving it under the condition that $p_3(0) = 0$, we get the equation for P_3

$$p_3(t) = \left\{ \lambda_{1,2}\lambda_{2,3} \mathrm{e}^{-\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t} \left[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)t} + \right.\right.$$
$$\left.\left. + \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \mathrm{e}^{\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t} + \left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{1,2}\right) \mathrm{e}^{\lambda_{1,2}t} \right] \right\} \Big/ \tag{7}$$
$$\Big/ \left[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{1,2}\right) \left(-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}+\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}\right) \right]$$

Substituting (7) into the fourth equation of the system (2) and solving it under the condition that $p_4(0) = 0$ we obtain the equation for P_4

$$p_4(t) = \left\{ \lambda_{1,2}\lambda_{2,3}\lambda_{3,4} \mathrm{e}^{-\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t} \left[-\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \times \right.\right.$$
$$\times \left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \times$$
$$\times \mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)t} + \left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \times$$
$$\times \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)t} -$$
$$- \left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \times \tag{8}$$
$$\times \mathrm{e}^{\lambda_{1,2}t} + \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \times$$
$$\left.\left. \times \left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \mathrm{e}^{\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t} \right] \right\} \Big/ \left[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \times \right.$$
$$\times \left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \times$$
$$\times \left(-\lambda_{1,2}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7}\right) \left(-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7}\right) \times$$
$$\left. \times \left(-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7}\right) \right]$$

By substituting (8) into the fifth equation of system (2) and solving it, taking into account the initial condition $p_5(0) = 0$, we will obtain a solution for P_5, which after a series of simplifications will have the form

$$p_5(t) = \lambda_{2,3}\lambda_{3,4}\lambda_{4,5} \Big/ \left[\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right) \left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}\right) \left(\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7}\right) \right] +$$
$$+ \left\{ \mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)t} \left[-\lambda_{1,2}\lambda_{2,3}\lambda_{3,4}\lambda_{4,5} \left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \times \right.\right.$$
$$\left.\left. \times \left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \right] \right\} \Big/ \left\{ \left(\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7}\right) \times \right.$$
$$\left. \times \left[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right) \left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right) \times \right.\right.$$
$$\left.\left. \times \left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right) \times \right.\right.$$
$$\ldots$$

$$\ldots$$
$$\times\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\Big]\Big\}+$$
$$+\Big\{\Big[\lambda_{1,2}\lambda_{2,3}\lambda_{3,4}\lambda_{4,5}\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right)\left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\times\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\Big]\mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)t}\Big\}\Big/\Big\{\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}\right)\times$$
$$\times\Big[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right)\left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\times$$
$$\times\left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\times\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\Big]\Big\}+\Big[\left(\lambda_{2,3}\lambda_{3,4}\,\lambda_{4,5}\times\right.$$
$$\times\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\left.\times\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\mathrm{e}^{\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\Big]+\Big\{\Big[1\Big/\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)\Big]\mathrm{e}^{\lambda_{1,2}t}\times\right.$$
$$\times\Big[-\lambda_{1,2}\lambda_{2,3}\lambda_{3,4}\lambda_{4,5}\left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\left.\times\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\Big]\Big\}\Big/\Big[\left(\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6}-\lambda_{2,7}\right)\times\right.$$
$$\times\left(\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6}-\lambda_{3,7}\right)\left(\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\times\left(\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\left(\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}-\lambda_{4,7}\right)\times$$
$$\left.\times\mathrm{e}^{\left(\lambda_{1,2}+\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}\right)t}\Big] \right. \tag{9}$$

Such an equation has a large number of discontinuities, since there are many points where the denominators in the terms of the function (9) become 0. For such points, you can use the approach given in (6) and obtain certain solutions of equation (9) at the discontinuity points:

$$\lambda_{1,2}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7};\ \lambda_{1,2}=\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7};\ \lambda_{1,2}=\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};$$
$$\lambda_{2,3}=-\lambda_{2,6}-\lambda_{2,7};\ \lambda_{2,3}=\lambda_{1,2}-\lambda_{2,6}-\lambda_{2,7};\ \lambda_{2,3}=-\lambda_{2,6}-\lambda_{2,7}+\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7};$$
$$\lambda_{2,3}=-\lambda_{2,6}-\lambda_{2,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};\quad \lambda_{2,6}=-\lambda_{2,3}-\lambda_{2,7};\quad \lambda_{2,6}=\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,7};$$
$$\lambda_{2,6}=-\lambda_{2,3}-\lambda_{2,7}+\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7};\quad \lambda_{2,6}=-\lambda_{2,3}-\lambda_{2,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};$$
$$\lambda_{2,7}=-\lambda_{2,3}-\lambda_{2,6};\quad \lambda_{2,7}=\lambda_{1,2}-\lambda_{2,3}-\lambda_{2,6};\quad \lambda_{2,7}=-\lambda_{2,3}-\lambda_{2,6}+\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7};$$
$$\lambda_{2,7}=-\lambda_{2,3}-\lambda_{2,6}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};\quad \lambda_{3,4}=-\lambda_{3,6}-\lambda_{3,7};\quad \lambda_{3,4}=\lambda_{1,2}-\lambda_{3,6}-\lambda_{3,7};$$
$$\lambda_{3,4}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,6}-\lambda_{3,7};\ \lambda_{3,4}=-\lambda_{3,6}-\lambda_{3,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};\ \lambda_{3,6}=-\lambda_{3,4}-\lambda_{3,7};$$
$$\lambda_{3,6}=\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,7};\ \lambda_{3,6}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,7}; \tag{10}$$
$$\lambda_{3,6}=-\lambda_{3,4}-\lambda_{3,7}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};\ \lambda_{3,7}=-\lambda_{3,4}-\lambda_{3,6};\ \lambda_{3,7}=\lambda_{1,2}-\lambda_{3,4}-\lambda_{3,6};$$
$$\lambda_{3,7}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{3,4}-\lambda_{3,6};\ \lambda_{3,7}=-\lambda_{3,4}-\lambda_{3,6}+\lambda_{4,5}+\lambda_{4,6}+\lambda_{4,7};\ \lambda_{4,5}=-\lambda_{4,6}-\lambda_{4,7};$$
$$\lambda_{4,5}=\lambda_{1,2}-\lambda_{4,6}-\lambda_{4,7};\ \lambda_{4,5}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,6}-\lambda_{4,7};$$
$$\lambda_{4,5}=\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,6}-\lambda_{4,7};\ \lambda_{4,6}=-\lambda_{4,5}-\lambda_{4,7};\ \lambda_{4,6}=\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,7};$$
$$\lambda_{4,6}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,7};\ \lambda_{4,6}=\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,7};\ \lambda_{4,7}=-\lambda_{4,5}-\lambda_{4,6};$$
$$\lambda_{4,7}=\lambda_{1,2}-\lambda_{4,5}-\lambda_{4,6};$$
$$\lambda_{4,7}=\lambda_{2,3}+\lambda_{2,6}+\lambda_{2,7}-\lambda_{4,5}-\lambda_{4,6};\ \lambda_{4,7}=\lambda_{3,4}+\lambda_{3,6}+\lambda_{3,7}-\lambda_{4,5}-\lambda_{4,6}$$

Function (9) is the target function of the "organization-insider" system. To achieve $p_5(t)\to 0$, it is necessary to find the corresponding values $\lambda_{i,j}$ on an interval

of time $t \to \infty$, since we are interested in the operation of the system in the stationary mode. It should be noted that the analytical solution of the optimization problem $p_5(t) \to \min$ is impossible due to the fact that then it will be necessary to impose a number of restrictions on most of the parameters $\lambda_{i,j}$. In this case, in order to achieve the goal of the work, it would be more appropriate to model equation (9).

Since we are not interested in the specific values $\lambda_{i,j}$ themselves, but only the ratio between $\lambda_{i,j}$, which refer to "attack" and "defense", then we will conduct a computational experiment in which we will investigate different values of these parameters. Recall that the intensity $\lambda_{1,2}$, $\lambda_{2,3}$, $\lambda_{3,4}$, $\lambda_{4,5}$ describe an insider attack and his/her ability to quickly operate in the organization's information system. Intensities $\lambda_{2,6}$, $\lambda_{3,6}$, $\lambda_{4,6}$ describe the capabilities of the organization's protection services, and $\lambda_{2,7}$, $\lambda_{3,7}$, $\lambda_{4,7}$ determine the technical protection capabilities due to the settings of Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM), etc., which do not give the insider the opportunity to realize his intentions.

A priori, we can imagine that to minimize the probability $p_5(t)$, it is necessary to achieve a certain ratio of intensities. In particular, considering the horizontal component of protection on each line, it is possible to distinguish the ratio of intensities, which can be formulated as follows:

$$\lambda_{2,6} + \lambda_{2,7} >> \lambda_{2,3}, \quad \lambda_{3,6} + \lambda_{3,7} >> \lambda_{3,4}, \quad \lambda_{4,6} + \lambda_{4,7} >> \lambda_{4,5} \tag{11}$$

The essence of inequalities (11) is that in order to create an effective line of defense against an insider threat, it is necessary to maximize the intensity of transitions to states 6 and 7 and minimize the insider transitioning to the next attack state (chain 1, 2, 3, 4, 5). The question of which line of defense is more expedient to achieve the maximum difference between intensities also remains interesting: do it as early as possible ($\lambda_{2,6} + \lambda_{2,7} >> \lambda_{2,3}$) or later ($\lambda_{3,6} + \lambda_{3,7} >> \lambda_{3,4}$ or $\lambda_{4,6} + \lambda_{4,7} >> \lambda_{4,5}$)?

So, let us take a sufficiently long time $t = 1\,000$ and, $\lambda_{1,2} = 1$ (since there is only one transition from state 1 to state 2) as initial conditions for simulation. Setting different values of intensities $\lambda_{i,j}$, and taking into account the constraints (10) to confirm the hypothesis (11), the corresponding values can be obtained $p_5(t)$. Simulation results for different intensity ratios $\lambda_{i,j}$ are shown in Fig. 3.

As we can see from Fig. 3*a* and 3*b*, for random values of attack intensities ($\lambda_{2,3}$, $\lambda_{3,4}$, $\lambda_{4,5}$) and protection intensities ($\lambda_{2,6}$, $\lambda_{2,7}$, $\lambda_{3,6}$, $\lambda_{3,7}$, $\lambda_{4,6}$, $\lambda_{4,7}$) over a significant period of time $t = 1\,000$, the probability of attack success is relatively insignificant. This is explained by the presence of three echelons of defense and the fact that the number of defensive transitions is twice as large as the number of offensive ones. In Fig. 3*c*, it can be seen that the absence of protection gives the maximum value of the attack success. An attack can be maximally successful ($p_5 \to 1$) in the case when the intensity of the attack is tens or hundreds of times higher than the intensity of the defense. The appearance of adequate protection (Fig. 3*d*) under the same conditions leads to a significant decrease in the success of the attack. It should be noted that only the ratio of intensities, and not their absolute value, will have the greatest influence on the success of the attack.

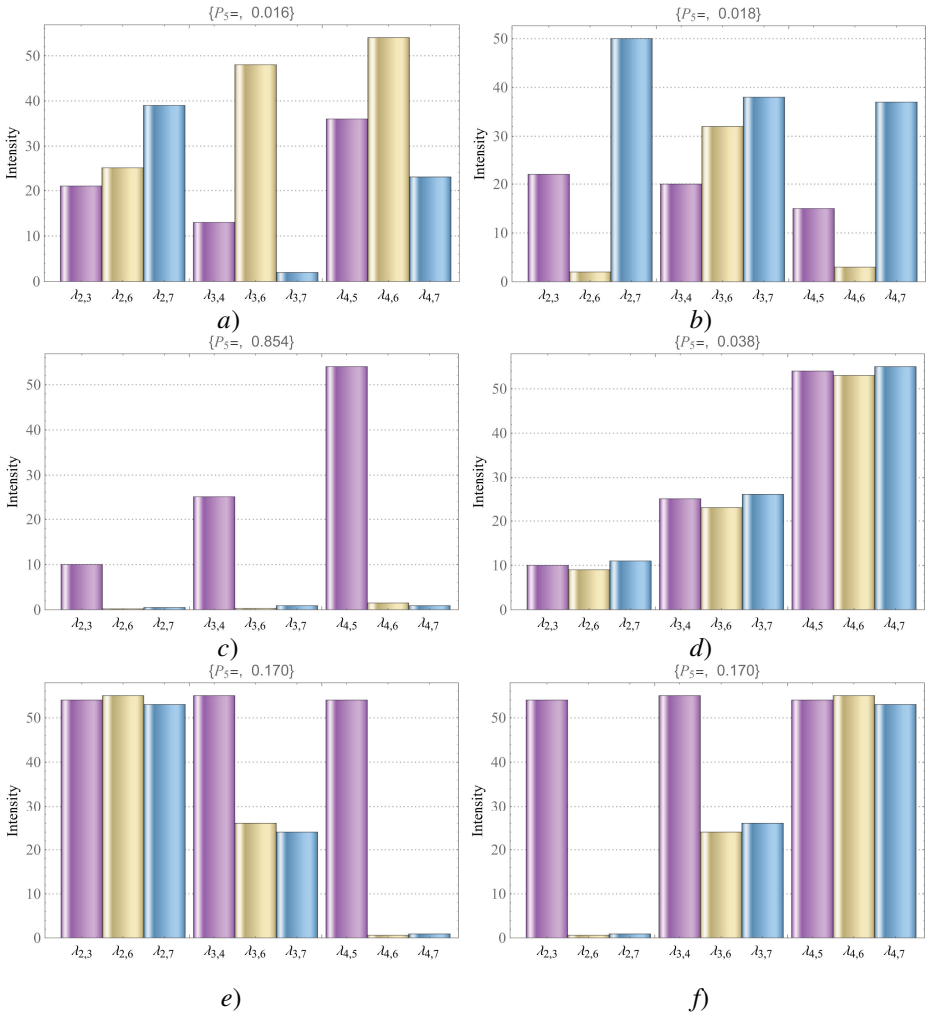

Fig. 3. Simulation results

And now let us analyze how the distribution of intensity between the defense echelons affects the success of the attack. Figs 3e and 3f show a symmetrical situation, when the main defense efforts are concentrated on the first echelon (Fig. 3*e* – risk analysis, preparation for an attack) or on the last echelon (Fig. 3*f* – removal of traces of influence). As you can see, in the first and second cases, the total probability of the insider reaching state 5 is the same ($p_5 = 0.170$). This again emphasizes that, within the framework of the model which is considered with the assumptions made, it is not so important where exactly the attack attempt is stopped. Of course, in real life, security services will try to neutralize the attacker as early as possible.

Taking into account the above experimental results it is possible to construct a general dependence of the probability of attack success on the average values of attack and defense intensities for the established modeling conditions (Fig. 4). Since it has already been established that it is not so important at which echelon the counterac-

tion is carried out and, with respect to the overall effect on the final probability, all echelons can be considered as a whole, then in this case the behavior of p_5 is investigated depending on the average intensity of the attack $\left(\lambda_{2,3}+\lambda_{3,4}+\lambda_{4,5}\right)/3$ and average protection intensity $\left(\lambda_{2,6}+\lambda_{2,7}+\lambda_{3,6}+\lambda_{3,7}+\lambda_{4,6}+\lambda_{4,7}\right)/6$.

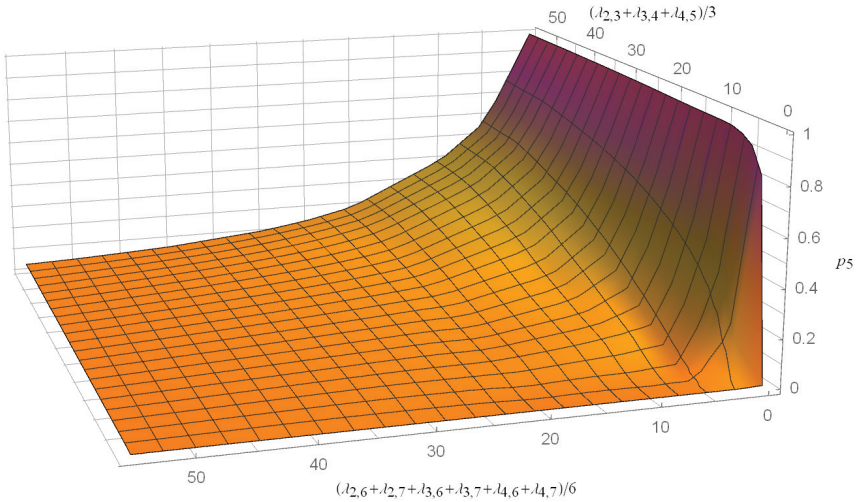

Fig. 4. Dependence of probability of achieving the goal by insider on ratio of intensities of insider and the protection system

It can be seen that as the intensity of the attack, which is determined by the insider's ability to penetrate further into the system to commit illegal actions, increases, the probability of reaching the desired state 5 increases rapidly. This is especially evident in the absence of a defense reaction. The appearance of protection almost immediately reduces the probability of success of the attack. In order to obtain a significant advantage in protection, the defense system must have the ability to respond tens or hundreds of times faster to the attempts of an insider's attack compared to an insider who puts forward a very real problem of selection and redistribution of employees to the heads of organizations.

As you can see, the main advantage of using Markov analysis to estimate the time parameters of an insider attack is that such an attack can be simulated quite simply. However, such a model is quite abstract and cannot cover all the nuances of an attack. Due to the fact that an increase in the number of states and transitions leads to an increase in the number of equations, we are forced to consider only the most basic states and transitions, which somewhat simplifies the model. In addition, in our case we assume that the intensities are time-independent variables, although in real life this is not always the case. Another disadvantage is caused by the essence of the Markov process, which assumes that for any moment in time, the probability of the system transitioning to the next state in the future depends only on the state the system is in now, and all previous states up to the current one are neglected. In the real world, there may be situations where the probability of transition to the next state will depend on some combination of previous states. Also, in our research, we focused on the marginal distribution of probabilities at $t \to \infty$, since we are interested in the state of the organization that would ensure the readiness of the defense system to counter an insid-

er attack at any time. All these disadvantages limit the detail and capabilities of Markov model for studying such a complex phenomenon as an insider attack.

5 Time Parameters of Counteraction to Insider Threat

Intensities $\lambda_{i,j}$ are inverse functions of time and the main attention should be focused on the time parameters of the system "organization – insider". The time-based approach to building information systems is not new, as a set of such factors is part of the key performance indicator (KPI) for IT incident management [13]. The publication [14] identified 7 key time indicators used in the construction of effective cybersecurity systems: 1) Alarm Time to Triage (TTT); 2) Alarm Time to Qualify (TTQ); 3) Threat Time to Invest (TTI); 4) Time to Mitigate (TTM); 5) Time to Recover (TTRv); 6) Incident Time to Detect (TTD); 7) Incident Time to Response (TTRs).

Considering the system "organization - insider", we can identify 2 key time factors (MTTD and MTTR) [15]:

- Mean Time to Detect (MTTD): Your MTTD is the average time it takes to detect a security threat or incident,
- Mean Time to Respond (MTTR): Your MTTR measures the average time it takes to control and remediate a threat.

MTTD and MTTR indicators depend on a number of factors, including the size and complexity of the organization's information network, the number and experience of IT staff, and so on. There are no standard approaches to measuring MTTD and MTTR, so detailed comparisons between organizations can be problematic.

Today, manufacturers of various IDS declare the possibility of reducing the time of detection of insider threats from a few tens of minutes to 1-2 minutes with the use of automation [16]. However, the problem of building a time-balanced system of protection against insider threats remains unsolved.

One of the promising ways to achieve a balance of time between the capabilities of a potential insider and the ability of security systems to detect it in a timely manner is previous work with Early Indicators. In [17], 21 key indicators were identified, which can be used to identify a potential insider in advance. This approach makes it possible to move from reactive security to proactive insider-threat risk reduction. Among such indicators, the authors note as the most important: 1) running software to enable sharing and access from remote machine; 2) opening a clear text file that potentially stores passwords; 3) exfiltrating a file to an unlisted USB device; 4) downloading file with potentially malicious extension; 5) exfiltrating tracked file to the web by uploading; etc.

It should be noted that calculating the attack and reaction time is quite a complicated task as it is difficult to measure the real-time of an attack or protection from an internal employee. In addition, such time indicators will significantly depend on the ability of specific performers to perform certain actions in the system. Moreover, because in organizations, information systems are significantly different, the time indicators will be significantly different. Also, the situation is complicated by the fact that organizations usually do not want to share such specific information.

Tab. 1 shows the time indicators collected according to the methodology [11] and the results of the analysis of communication with representatives of security services of different organizations. These indicators are only an option and do not claim absolute completeness. It is assumed that the next transition can be made when the previous transition has already been performed.

Tab. 1 Time indicators of insider threat mitigation

Intensity	Components of time	Time
$\lambda_{1,2} = \frac{1}{\overline{t}_{1,2}}$	$\overline{t}_{1,2} = \overline{t}_{1,2,1} + ... + \overline{t}_{1,2,n}$ – the time during which the employee intends to commit illegal acts (normal operation; work with intentions of revenge or illegal activity; suspicious contacts; disgruntlement; exposed to temptation; change in personal life; applying for promotions/job changes).	3-5 years – for a casual insider. 3-6 weeks – for a malicious insider.
$\lambda_{2,3} = \frac{1}{\overline{t}_{2,3}}$	$\overline{t}_{2,3} = \overline{t}_{2,3,1} + ... + \overline{t}_{2,3,n}$ – the time for the insider to study the situation and prepare for the attack (determine the attack targets; collect information; identify vulnerabilities in security system; searching through data or contacting people for info/help not applicable to job; suspicious requests; malicious access).	3-5 days
$\lambda_{3,4} = \frac{1}{\overline{t}_{3,4}}$	$\overline{t}_{3,4} = \overline{t}_{3,4,1} + ... + \overline{t}_{3,4,n}$ – the time of insider attack (penetration into the object; unauthorized access; search for target data; data verification; copying data; collecting data in a centralized place).	1-3 hours
$\lambda_{4,5} = \frac{1}{\overline{t}_{4,5}}$	$\overline{t}_{4,5} = \overline{t}_{4,5,1} + ... + \overline{t}_{4,5,n}$ – the time of the attack traces destruction by the insider (deleting logs; destroying physical evidence).	1-2 hours
$\lambda_{2,6} = \frac{1}{\overline{t}_{2,6}}$	$\overline{t}_{2,6} = \overline{t}_{2,6,1} + ... + \overline{t}_{2,6,n}$ – the time of detection and interception of the insider by the security service in preparation for the attack (searching through data or contacting people for info not applicable to the job; suspicious requests not compliant with company policy; malicious unapproved access).	4-7 days
$\lambda_{3,6} = \frac{1}{\overline{t}_{3,6}}$	$\overline{t}_{3,6} = \overline{t}_{3,6,1} + ... + \overline{t}_{3,6,n}$ – the time of detection and interception of the insider by the security service during the attack (requesting staff overlook responsibilities; hiding files).	1-2 hours, if security is detected by unapproved access
$\lambda_{4,6} = \frac{1}{\overline{t}_{4,6}}$	$\overline{t}_{4,6} = \overline{t}_{4,6,1} + ... + \overline{t}_{4,6,n}$ – the time of interception of the insider by the security service at the stage of destruction of traces (deleting logs/IT evidence; destroying physical evidence; impersonation/ masquerading).	30-60 min, in case of detection by security service
$\lambda_{2,7} = \frac{1}{\overline{t}_{2,7}}$	$\overline{t}_{2,7} = \overline{t}_{2,7,1} + ... + \overline{t}_{2,7,n}$ – the time required for the insider to decide whether to take further action in preparation for the attack (detection of malware; downloading/writing/installing by IDS; detection of unauthorized access by IDS; detection of privilege escalation by IDS).	1-2 days if IDS can detect all attempts to prepare for an attack
$\lambda_{3,7} = \frac{1}{\overline{t}_{3,7}}$	$\overline{t}_{3,7} = \overline{t}_{3,7,1} + ... + \overline{t}_{3,7,n}$ – the time required for the insider to decide whether to take further action during the attack phase (detection of external exfiltration by IDS).	20-40 min if IDS detects unapproved access
$\lambda_{4,7} = \frac{1}{\overline{t}_{4,7}}$	$\overline{t}_{4,7} = \overline{t}_{4,7,1} + ... + \overline{t}_{4,7,n}$ – the time required for the insider to decide whether to take further action at the stage of destroying the traces (deleting logs/IT evidence; impersonation/masquerading; destroying physical evidence).	10-20 min if IDS detects an exfiltration attempt

Thus, it is better to operate with the ratio of time between individual performers. The ratio of time can be determined both at the stage of hiring an employee and in the process of his professional activity. The recruitment stage is more reliable, because in order to get a job the employee will have to demonstrate their real capabilities. For more effective evaluation, HR employees need to compose tasks in such a way that they reflect a real-time picture of the job applicant's activities. The list of questions can be made, as for example in [18], providing at the same time practical tasks for their decision.

However, this approach may not shed light on the real picture because:

- an employee who is just applying for a job may not have sufficient skills to work with the necessary tools,
- in the process of work, the employee can obtain the necessary skills and qualifications through self-study,
- specific time indicators of an individual employee should be compared with others, including already working employees of the organization.

You can use the method of pairwise comparisons to display the task time rating for each employee of the organization. Each already working employee is evaluated by his boss in comparison with another employee according to certain criteria of speed of performance of certain tasks. As a result of applying the method, you can get a rating of employees who will be ranked by the speed of working with information resources. Other factors must also be considered, including the ability to independently develop and install software.

It is especially important to compare the capabilities of employees with representatives of the security services of the organization. The required intensity ratio (11) can only be achieved when safety workers respond to system events much faster (less response time) than other workers.

6 Conclusion

Despite the large number of publications devoted to mitigating the insider threat published so far, only insufficiently effective models for describing an insider attack have been developed. Among the factors that have the greatest impact on the threat mitigation process, one of the most decisive is time.

The organization's security system, built on the concept of a balanced response time of the defense to the actions of a potential insider, is the most promising model of threat mitigation. It is necessary to achieve such a ratio of the time that the attacker will spend on the attack and the time for which the security system will be able to identify it, so that the security system is ahead of any possible actions of the insider.

In the practical implementation of the proposed approach, a system of control of practical skills of employees to work with any information resources of the organization should be created. Resources spent on protection should be more productive than the resources of basic information systems. The staff of security services should be more qualified than the main staff of the organization. Since the physical resources and qualifications of employees are constantly changing, this model of security system must work constantly.

The direction of further research can be a wide range of issues to determine the time indicators of the proposed model. In particular, criteria and methods for automated assessment of the capabilities of the organization's staff should be developed in order to maintain the necessary balance of time working with information resources.

References

[1] STORCHAK, Y. *Insider Threat Statistics for 2024: Reports, Facts, Actors, and Costs* [online]. 2024 [viewed 2024-03-19]. Available from: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

[2] AL-MHIQANI, M., A. RABIAH, Z.A. ZAHEERA, M. WARUSIA, H. ASLINDA, A. KARRAR, A. NABEEL and Y. ZAHRI. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences,* 2020, **10**(15), 5208. DOI 10.3390/app10155208.

[3] KORNIYENKO, B.Y., L. GALATA and L. LADIEVA. Mathematical Model of Threats Resistance in the Critical Information Resources Protection System. In: *International Conference on Intelligent Tutoring Systems* [online]. Kingston: ITS, 2019 [viewed 2023-07-05]. Available from: https://ceur-ws.org/Vol-2577/paper23.pdf

[4] NONG, Y., Z. YEBIN and B. CONNIE. Robustness of the Markov-Chain Model for Cyber-Attack Detection. *IEEE Transactions on Reliability,* 2004, **53**(1), pp. 116-123. DOI 10.1109/TR.2004.823851.

[5] KASENOV, A.A., E.F. KUSTOV, A.A. MAGAZEV and V.F. TSYRULNIK. A Markov Model for Optimization of Information Security Remedies. *Journal of Physics: Conference Series*, 2020, **1441**, 012043. DOI 10.1088/1742-6596/1441/1/012043.

[6] QISI, L., X. LIUDONG and Z. CHENCHENG. Probabilistic Modeling and Analysis of Sequential Cyber-Attacks. *Engineering Reports,* 2019, **1**(4), e12065. DOI 10.1002/eng2.12065.

[7] LE, N. and H. DOAN. A Threat Computation Model Using a Markov Chain and Common Vulnerability Scoring System and its Application to Cloud Security. *Journal of Telecommunications and the Digital Economy,* 2019, **7**(1), pp. 37-56. DOI 10.18080/jtde.v7n1.181.

[8] MAGAZEV, A. and V. TSYRULNIK. On Small Perturbations of Markov Cyber Threat Models. *Journal of Physics: Conference Series,* 2021, **1745**, 012111. DOI 10.1088/1742-6596/1745/1/012111.

[9] LOCKHEED M. *Cyber Kill Chain* [online]. 2021 [viewed 2023-07-05]. Available from: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[10] *MITRE ATT&CK®* [online]. [viewed 2023-07-05]. Available from: https://attack.mitre.org/

[11] READ, D., A. ALAMIR, S. DUGDALE, N. STRIDE and D. LOBO. *Introducing the Insider Attack Matrix* [online]. 2021 [viewed 2023-07-05]. Available from: https://www.gresearch.co.uk/article/introducing-the-insider-attack-matrix/

[12] BARROS, A. *Applying the MITRE ATT&CK Framework to Detect Insider Threats* [online]. 2021 [viewed 2023-07-05]. Available from: https://www.brighttalk.com/webcast/15533/455015/applying-the-mitre-att-ck-framework-to-detect-insider-threats

[13] PASCUCCI, M. *What You Should Know About Driving Down MTTD and MTTR* [online]. 2021 [viewed 2023-07-05]. Available from: https://www.ccsinet.com/blog/driving-down-mttd-mttr/

[14] CHENG, Y., J. DENG, J. LI, S. DELOACH, A. SINGHAL and X. OU. Metrics of Security. In: A. KOTT, C. WANG and R.F. ERBACHER, eds. *Cyber Defense and Situational Awareness.* Cham: Springer, 2014, pp. 263-295. ISBN 978-3-319-11390-6.

[15] *MTTD and MTTR: Two Metrics to Improve Your Cybersecurity* [online]. 2020 [viewed 2023-07-05]. Available from: https://threatpost.com/mttd-and-mttr-two-metrics-to-improve-your-cybersecurity/152149/

[16] *Best Insider Threat Management (ITM) Software* [online]. 2024 [viewed 2024-03-19]. Available from: https://www.g2.com/categories/insider-threat-management-itm

[17] *Why Early Indicators of Insider Threat Risk Are So Valuable – And Which Ones to Use* [online]. 2020 [viewed 2023-07-05]. Available from: https://www.proofpoint.com/us/blog/insider-threat-management/why-early-insider-threat-indicators-are-so-valuable

[18] *Global Guideline – Interviewer and Interviewee Guide* [online]. 2022. [viewed 2023-07-05]. Available from: https://www.globalguideline.com/interview_questions/