Mathematical Modelling of the Process for Impact on Automated Information System Security of Threats Access to Restricted Information

Alexandr P. Rosenko
Department of applied mathematics and computer security
North Caucasus University,
Stavropol,
Russian Federation
pmkb.ncfu@gmail.com

Evgeniya A. Nekrasova
Department of applied mathematics and computer security
North Caucasus University,
Stavropol,
Russian Federation
ne-myza@yandex.ru

Abstract

This paper presents the results of mathematical modeling of influence of various dependent threats on security of information with restricted access. The article proposes a method and software implementation in relation to the particular case, namely the impact on automated information system (AIS) of two dependent threats. The method is based on application of Markov stochastic processes with discrete states and there are recommendations for optimizing the process of protecting information of restricted access in terms of the stochastic of a successful outcome from the automated information system of internal and external threats in this method in accordance with the results of mathematical modeling.

1 Introduction

There is much attention to the questions of information security for restricted access from both domestic and foreign researches in scientific and technical literature. For these purpose, different scientific approaches are used related to the development of mathematical models and mathematical modeling.

This is due to the tendency of many researches to describe more accurately the diversity of situations the impact of restricted information on various threats, taking into account the description of the greatest possible number of factors influencing safety information.

However, it should be noted the limitations of these approaches, since most of the them allow to explore the issue of protecting information on the qualitative level.

Studies show, that for the quantification of information security of restricted access widely used Markov random processes with discrete and continuous state.

Dependence of internal threats can be illustrated by the following example: programmer error in software product creation process does not depend on the unauthorized removal of restricted access information through

In: S. Hölldobler, A. Malikov, C. Wernhard (eds.): *YSIP2 – Proceedings of the Second Young Scientist's International Workshop on Trends in Information Processing, Dombai, Russian Federation, May 16–20, 2017*, published at http://ceur-ws.org.

the implementation of the programmed bookmark, but generates it, and vice versa when the unauthorized removal of information with restricted access through programmatic bookmarks arises regardless of the erroneous actions of a programmer, but generates it.

In this paper it is shown that the automated information system refers to complex stochastic man-machine systems that quantify information security can be restricted through the use of automated information systems of Markov stochastic processes.

2 Development of a method for assessing dependent threats on security of information with restricted access, circulating in an automated information system

Consider a situation, where a system is affected by two dependent threat, as shown in fig. 1, that can be mutually with probabilities, r_{12} and r_{21}. Denoted by q_1 and q_2 the likelihood of the first and second threat (fig. 1). Parrying first and second threat occurs with probability R_1 and R_2, probabilities not parrying, with probabilities, $\overline{R}_{13}$ and $\overline{R}_{23}$

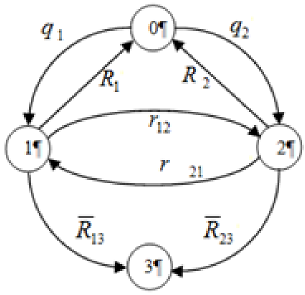


Figure 1: Condition graph of an automated information system under the influence of two independent threats

The system can be in the following conditions: condition "0" – internal threats do not appear; condition "1" – the first threat is manifested with intensity q_1 and her parrying becomes with probability R_1 as can be seen in the figure 1. A successful parrying convert automated information system of the condition the "1" in the original zero condition; condition the "2" – the second threat is manifested with probability q_2 and her parrying and transition zero condition is done with probability R_2 condition the "3" – absorbing condition. In this condition the system can go from a condition of "1" with probability $\overline{R}_{13}$ and out of "2" with probability $\overline{R}_{23}$ Absorbing condition characterizes leak the information of restricted access as a result of the implementation of the attacker dependent threats [Ros10].

Matrix of probabilities for transitions of systems from condition to condition can be represented as follows as can be seen in the figure 1:

$$||P_{ij}|| = \begin{vmatrix} 1-q_{\sum} & q_1 & q_2 & 0 \\ R_1 & 0 & r_{12} & \overline{R}_{13} \\ R_2 & r_{21} & 0 & \overline{R}_{23} \\ 0 & 0 & 0 & 1 \end{vmatrix} \tag{1}$$

Applying previously proposed methodology [Ros10] for primary source data, the relevant probabilities $P_1(0) = P_2(0) = P_3(0) = 0$ after the first step, the probability will be equal conditions:

$$P_0(2) = \left(1-q_{\sum}\right)^2 + q_1R_1 + q_2R_2, P_1(2) = \left(1-q_{\sum}\right)q_1 + q_2r_{21}, P_2(2) = \left(1-q_{\sum}\right)q_2 + q_1r_{12}; \tag{2}$$

The likelihood of condition after second step:

$$P_0(2) = \left(1-q_{\sum}\right)^2 + q_1R_1 + q_2R_2, P_1(2) = \left(1-q_{\sum}\right)q_1 + q_2r_{21}, P_2(2) = \left(1-q_{\sum}\right)q_2 + q_1r_{12};$$

$$P_3(2) = q_1\overline{R}_{13} + q_2\overline{R}_{23} \tag{3}$$

Then the probability of the unfavorable outcome is determined as follows:

$$Q_{SO}(2) = 1 - P_{SO}(2) = P_3(2) or Q_{SO}(2) = q_{01}\overline{R}_{13} + q_{02}\overline{R}_{23}. \tag{4}$$

The probability of the condition of the system after the third step will be of the form:

$$P_0(3) = \left(1 - q_{\sum}\right)^3 + \sum_{i=1}^{2} q_{0i}R_{i0} + \left(1 - q_{\sum}\right)(q_{01}R_{10} + q_{02}R_{20}) + q_{02}r_{21}R_{10} + q_{01}r_{12}R_{20}, \tag{5}$$

$$P_1(3) = \left[\left(1 - q_{\sum}\right)^2 + \sum_{i=1}^{2} q_{0i}R_{i0}\right] q_{01} + \left[\left(1 - q_{\sum}\right) q_{02} + q_1 r_{12}\right] * r_{21}, \tag{6}$$

$$P_2(3) = \left[\left(1 - q_{\sum}\right)^2 + \sum_{i=1}^{2} q_{0i}R_i\right] q_{02} + \left[\left(1 - q_{\sum}\right) q_{01} + q_{02}r_{21}\right] r_{12}, \tag{7}$$

$$P_3(3) = \left[\left(1 - q_{\sum}\right) q_{01} + q_{02}r_{21}\right] \overline{R}_{13} + \left[\left(1 - q_{\sum}\right) q_{02} + q_{01}r_{12}\right] \overline{R}_{23}. \tag{8}$$

After the third step of transformation the likelihood of a successful outcome from the impact on the system is equal to the

$$P_{BI}(3) = P_0(3) + P_1(3) + P_2(3), \tag{9}$$

and the opposite event unsuccessful outcome, i.e. determined by the ratio of

$$Q_{SO}(3) = P_3(3). \tag{10}$$

Use obtained dependencies for determine the likelihood of a successful outcome taking into account the impact on automated information system dependent threats.

It should be noted that the assessment procedure will be continued by increasing the number of moves and, thus, complicating the assessment algorithm [Lei13].

This can be clearly point out the obvious pattern that as you increase the number of steps increases and the probability of the unsuccessful outcome of the from the automated information system dependent threats.

3 Mathematical modelling of the process of impact two dependent threats on automated information system

Modeling of impact on automated information system two dependent threats in accordance with figure 1 and a matrix of condition (1).

Basic data for the calculation:

$$P_0(0) = 1; P_1(0) = P_2(0) = P_3(0) = 0; \tag{10}$$

the likelihood of the first threat varies from $q_1 = 0,0$ to $q_1 = 0.8$ the probability of the second internal threat $q_2 = 0.2$;

the likelihood of parrying second internal threat $R_2 = 0.2$, the likelihood of mutual spawn internal threats $r_{12} = r_{21} = 0.2$.

Parrying chance by internal threats $R_1 = 0.2$.

Since the condition from figures should be: the system may be in absorbing condition after the second and subsequent steps; with the increase in the probability of the internal threat the probability of a transition system in absorbing condition increases. However, on the nature of the changes specified probability significant influence has the likelihood of parrying emerging threats.

So, for example, on the fifth step of calculation for $R_1 = 0.2$ the probability that the system reaches the absorbing condition, provided that the probability of $q_1 = 0.0$ to $q_1 = 0.08$, respectively: 0.43; 0.63; 0.83; 0.88 and 0.91, whereas if you increase these probabilities up 0.6 R_1 for similar probabilities of q_1 respectively, have the following meanings: 0.4; 0.48; 0.55; 0.59 and 0.62.

Also shows that with increasing probability of 0.2 to 0.6 R_1 steady degeneration charts built for values between $q_1 = 0.2$ to $q_1 = 0.8$ with the timetable for $q_1 = 0.0$; simulation results show that the graph for $q_1 = 0.8$

practically does not change their situation with rising R_1 (loosely pronounced growth trend); It can be shown that if $R_1 \to 1.0$ graphics when you change the setting of the schedule if $q_1 = 0.0$.

The specified probability is defined for the source data, discussed in the first and second task except that in this case changed the probability parrying a second displayed threats from $R_2 = 0.4$ to $R_2 = 0.6$ and R_1 is fixed to the value $R_1 = 0.2$.

Analysis of the results of the simulation allows the following conclusions to be drawn: with the increasing likelihood of R_2 is observed slight increase the likelihood of successful outcome from exposure to the automated information system of internal threats throughout the range of changes to the parameter q_1 , i.e. if you change the $q_1 = 0.0/0.8$;

The analysis also shows the absence of degeneration of the graphs if you are changing the settings for q_1 and R_2, that reflects the positive impact of parameter R_2 on the likelihood of successful outcome across the whole range of changes to the parameter q_1

Thus, the simulation results show that for similar source data with the increasing likelihood of parrying manifested first threat i.e. R_1 all graphics are approaching to graph, obtained for $q_1 = 0.0$

With increased R_2 all graphics smoothly move in the direction of increasing the likelihood of a successful outcome from the effects of internal threats to the automated information system.

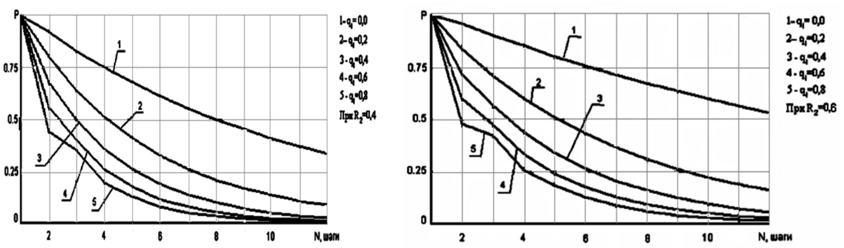
This suggests that the owner information of restricted access can realize different ways to use safeguard mechanisms. Depending on the available material resources he can realize those gives best effect positive. The system may be in absorbing condition after the second and subsequent steps. The probability of a transition system in absorbing condition increases with increasing probability of the internal threat. However, on the nature of the changes the specified probability significant influence has the likelihood of parrying emerging threats.

So, for example, on the fifth step of calculation for $R_1 = 0.2$ the probability that the system reaches the absorbing State, provided that the probability of $q_1 = 0.0$ to $q_1 = 0.08$, respectively: 0.43; 0.63; 0.83; 0.88 and 0.91, while if you increase these probabilities up R_1 to 0.6 for similar probabilities of q_1 respectively, have the following meanings: 0.4; 0.48; 0.55; 0.59 and 0.62. Also shows that with increasing probability R_1 of 0.2 to 0.6 steady convergence graphs constructed from values $q_1 = 0.2$ to $q_1 = 0.8$ with the graph for $q_1 = 0.0$;

Simulation results show that the graph for $q_1 = 0.0$, practically does not change their situation with rising R_1 (loosely pronounced growth trend);

It can be shown that when $R_1 \to 1.0$ graphics when you change a parameter $q_1 = 0.2/0.8$ merge with the timetable if $q_1 = 0.0$

The specified probability is defined for the source data, discussed in the first and second task, except that in this case changed the likelihood of parrying second manifested threats from $R_2 = 0.4$ to $R_2 = 0.6$, and R_1 is fixed with value $R_2 = 0.2$. Simulation results are presented in figure 2. a) ($R_2 = 0.4$) and b) ($R_2 = 0.6$)



a) b)

Figure 2: The dependence of the probability of a successful outcome from the automated information system of two dependent internal threats ($R_1 = 0.2$)

Analysis of modelling results presented in figure 2 a) and b) leads to the following conclusions:

With the increased probability R_2 of slight growth probability successful outcome from exposure on the automated information system internal threats throughout the range of changes to the parameter q_1 i.e. at change $q_1 = 0.0/0.8$

The analysis also shows the lack of convergence graphs when you change the parameters q_1 and R_2, indicating the positive effect of parameter on the likelihood of a successful outcome of the R_2 in all range of parameter changes q_1.

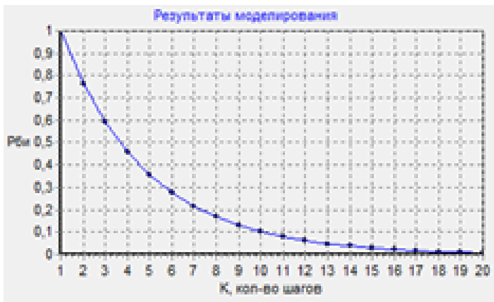
Thus, the simulation results show that for similar source data with increase the probability parrying of the first threat like R_1, all graphics are approaching the graphics obtained for $q_1 = 0.0$ With increased R_2 all graphics smoothly move in the direction of increasing the likelihood of a successful outcome from the effects of internal threats to the automated information system. This suggests that the owner information of restricted access may apply are different ways to use safeguard mechanisms. Depending on the available material resources he can realize those of them, that give best effect positive.

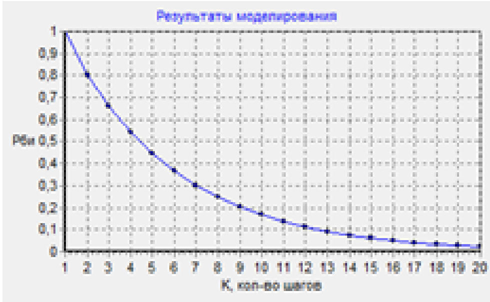
3.1 Study of the influence of parrying settings threats by the likelihood of a successful outcome

Let carry out a simulation of a quantitative assessment of information security, limited access to the research of influence of parrying settings threats by the likelihood of a successful outcome. Consider one set of inputs, which would change the magnitude of probabilities parrying threats.

Prepare the table tests:

Table 1: Testing the influence of Parrying threats, probabilities to the likelihood of a successful outcome

<table>
<tr><th></th><th>Matrix of transition probabilities</th><th>graph of dependence of successful outcome P_{SO} of the number of steps the algorithm</th><th>Probabilities parrying threats, R</th></tr>
<tr><td>1</td><td><table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr>
<tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr>
<tr><td>P1</td><td>0,1</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,8</td></tr>
<tr><td>P2</td><td>0,1</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,8</td></tr>
<tr><td>P3</td><td>0,1</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,8</td></tr>
<tr><td>P4</td><td>0,1</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,8</td></tr>
<tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table></td><td>
</td><td>0.1</td></tr>
<tr><td>2</td><td><table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr>
<tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr>
<tr><td>P1</td><td>0,2</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,7</td></tr>
<tr><td>P2</td><td>0,2</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,7</td></tr>
<tr><td>P3</td><td>0,2</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,7</td></tr>
<tr><td>P4</td><td>0,2</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,7</td></tr>
<tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table></td><td>
</td><td>0.2</td></tr>
<tr><td>3</td><td><table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr>
<tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr>
<tr><td>P1</td><td>0,3</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,6</td></tr>
<tr><td>P2</td><td>0,3</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,6</td></tr>
<tr><td>P3</td><td>0,3</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,6</td></tr>
<tr><td>P4</td><td>0,3</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,6</td></tr>
<tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table></td><td>
</td><td>0.3</td></tr>
</table>

<table>
<tr><td>4</td><td><table><tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr><tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr><tr><td>P1</td><td>0,4</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,5</td></tr><tr><td>P2</td><td>0,4</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,5</td></tr><tr><td>P3</td><td>0,4</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,5</td></tr><tr><td>P4</td><td>0,4</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,5</td></tr><tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>
</td><td>0.4</td></tr>
<tr><td>5</td><td><table><tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr><tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr><tr><td>P1</td><td>0,5</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,4</td></tr><tr><td>P2</td><td>0,5</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,4</td></tr><tr><td>P3</td><td>0,5</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,4</td></tr><tr><td>P4</td><td>0,5</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,4</td></tr><tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>
</td><td>0.5</td></tr>
<tr><td>6</td><td><table><tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr><tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr><tr><td>P1</td><td>0,6</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,3</td></tr><tr><td>P2</td><td>0,6</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,3</td></tr><tr><td>P3</td><td>0,6</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,3</td></tr><tr><td>P4</td><td>0,6</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,3</td></tr><tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>
</td><td>0.6</td></tr>
<tr><td>7</td><td><table><tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr><tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr><tr><td>P1</td><td>0,7</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,2</td></tr><tr><td>P2</td><td>0,7</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,2</td></tr><tr><td>P3</td><td>0,7</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,2</td></tr><tr><td>P4</td><td>0,7</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,2</td></tr><tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>
</td><td>0.7</td></tr>
<tr><td>8</td><td><table><tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr><tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr><tr><td>P1</td><td>0,8</td><td>0</td><td>0,03</td><td>0,04</td><td>0,03</td><td>0,1</td></tr><tr><td>P2</td><td>0,8</td><td>0,02</td><td>0</td><td>0,07</td><td>0,01</td><td>0,1</td></tr><tr><td>P3</td><td>0,8</td><td>0,01</td><td>0,05</td><td>0</td><td>0,04</td><td>0,1</td></tr><tr><td>P4</td><td>0,8</td><td>0,02</td><td>0,02</td><td>0,06</td><td>0</td><td>0,1</td></tr><tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr></table></td><td>
</td><td>0.8</td></tr>
</table>

<table>
<tr>
<td>9</td>
<td>
<table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th><th>P5</th></tr>
<tr><td>P0</td><td>0,6</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0,1</td><td>0</td></tr>
<tr><td>P1</td><td>0,95</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0,05</td></tr>
<tr><td>P2</td><td>0,95</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0,05</td></tr>
<tr><td>P3</td><td>0,95</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0,05</td></tr>
<tr><td>P4</td><td>0,95</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0,05</td></tr>
<tr><td>P5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td>
<td>
</td>
<td>0.95</td>
</tr>
</table>

Based on data of table 1, build graph modeling outcomes with different probabilities Parrying threats, the results are presented in figure 3.

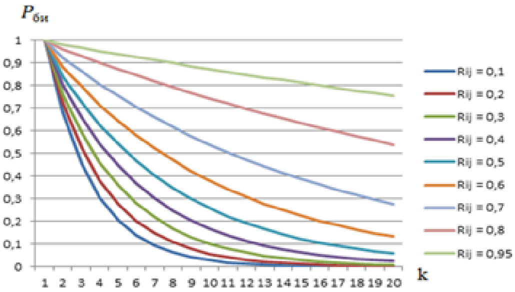


Figure 3: graph of dependence of successful outcome of P_{so} of the number of steps the algorithm with different probabilities Parrying threats

In conclusion with the results of figure 1:

Probability of P_{SO} successful outcome from exposure to automated information system dependent threats largely depends on the probabilities parrying dependent threats. The more likelihood of parrying dependent threats, the slower the P_{SO} decreases, and therefore the automated information system containing restricted information is more secure;

With the increase in the probability of the dependent threats the likelihood of an automated information system in the absorbing state is increased. Nature changes the specified probability depends on the probabilities Parrying discovered dependent threats;

Mathematical simulation results indicate that the owner information of restricted access, there are different ways to use protective equipment. Depending on the available material resources, it can implement the ones that give a positive result.

3.2 Study of the influence of mutual threats emit parameters by the likelihood of a successful outcome

Let carry out a simulation of a quantitative assessment of information security of restricted access, for research on the effect of mutual threats emit parameters on the value of the probability of a successful outcome. Consider one set of inputs, which would change the magnitude of probabilities of mutual threats emit.

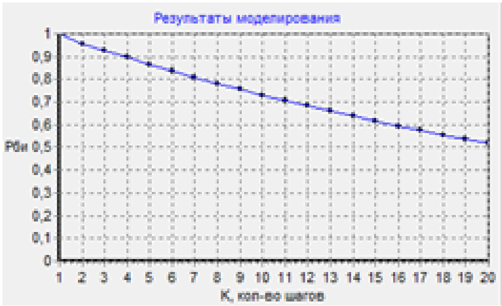
Prepare the table tests:

Table 2: Test of influence of probabilities of mutual threats emit on the likelihood of a successful outcome

	Matrix of transition probabilities	graph of dependence of successful outcome P_{SO} of the number of steps the algorithm	The likelihood of mutual threats

1

	P0	P1	P2	P3	P4
P0	0,7	0,05	0,1	0,15	0
P1	0,8	0	0	0	0,2
P2	0,9	0	0	0	0,1
P3	0,85	0	0	0	0,15
P4	0	0	0	0	1



0.0

2

	P0	P1	P2	P3	P4
P0	0,7	0,05	0,1	0,15	0
P1	0,7	0	0,05	0,05	0,2
P2	0,8	0	0,05	0,05	0,1
P3	0,75	0,05	0	0,05	0,15
P4	0	0	0	0	1

0.05

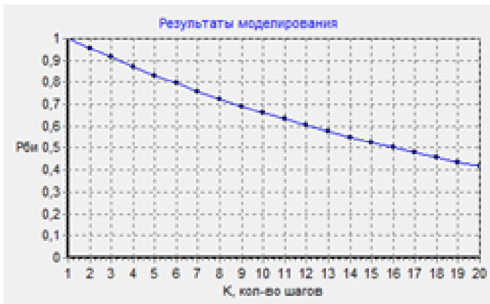
3

	P0	P1	P2	P3	P4
P0	0,7	0,05	0,1	0,15	0
P1	0,6	0	0,1	0,1	0,2
P2	0,7	0	0,1	0,1	0,1
P3	0,65	0,1	0	0,1	0,15
P4	0	0	0	0	1

0.1

4

	P0	P1	P2	P3	P4
P0	0,7	0,05	0,1	0,15	0
P1	0,5	0	0,15	0,15	0,2
P2	0,6	0	0,15	0,15	0,1
P3	0,55	0,15	0	0,15	0,15
P4	0	0	0	0	1



0.15

5

	P0	P1	P2	P3	P4
P0	0,7	0,05	0,1	0,15	0
P1	0,4	0	0,2	0,2	0,2
P2	0,5	0	0,2	0,2	0,1
P3	0,45	0,2	0	0,2	0,15
P4	0	0	0	0	1

0.2

<table>
<tr>
<td>6</td>
<td>
<table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th></tr>
<tr><td>P0</td><td>0,7</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0</td></tr>
<tr><td>P1</td><td>0,3</td><td>0</td><td>0,25</td><td>0,25</td><td>0,2</td></tr>
<tr><td>P2</td><td>0,4</td><td>0</td><td>0,25</td><td>0,25</td><td>0,1</td></tr>
<tr><td>P3</td><td>0,35</td><td>0,25</td><td>0</td><td>0,25</td><td>0,15</td></tr>
<tr><td>P4</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td>
<td>
</td>
<td>0.25</td>
</tr>
<tr>
<td>7</td>
<td>
<table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th></tr>
<tr><td>P0</td><td>0,7</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0</td></tr>
<tr><td>P1</td><td>0,2</td><td>0</td><td>0,3</td><td>0,3</td><td>0,2</td></tr>
<tr><td>P2</td><td>0,3</td><td>0</td><td>0,3</td><td>0,3</td><td>0,1</td></tr>
<tr><td>P3</td><td>0,25</td><td>0,3</td><td>0</td><td>0,3</td><td>0,15</td></tr>
<tr><td>P4</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td>
<td>
</td>
<td>0.3</td>
</tr>
<tr>
<td>8</td>
<td>
<table>
<tr><th></th><th>P0</th><th>P1</th><th>P2</th><th>P3</th><th>P4</th></tr>
<tr><td>P0</td><td>0,7</td><td>0,05</td><td>0,1</td><td>0,15</td><td>0</td></tr>
<tr><td>P1</td><td>0,1</td><td>0</td><td>0,35</td><td>0,35</td><td>0,2</td></tr>
<tr><td>P2</td><td>0,2</td><td>0</td><td>0,35</td><td>0,35</td><td>0,1</td></tr>
<tr><td>P3</td><td>0,15</td><td>0,35</td><td>0</td><td>0,35</td><td>0,15</td></tr>
<tr><td>P4</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td>
<td>
</td>
<td>0.35</td>
</tr>
</table>

Graph of results can be constructed with the results of table 2 emit the results are presented in figure 4.

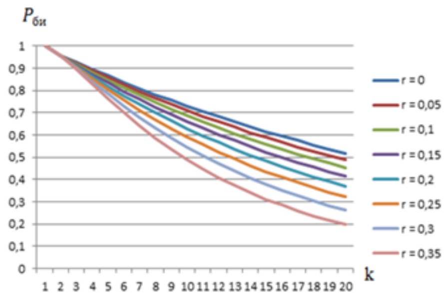


Figure 4: graph of dependence of successful outcome of P_{SO} of the number of steps the algorithm with different probabilities of mutual threats

In conclusion with the results of figure 4:

Probability P_{SO} of successful outcomes for the automated information system, from exposure to the threats of information with restricted access depends on the probabilities of mutual threats. The more the likelihood of mutual threats emit, the faster the decreases P_{SO} and therefore the automated information system with high probabilities of mutual threats will emit less secure

The presence of the owner information of restricted access results of mathematical modelling allows him to take science-based activities protection of existing information resources.

4 Conclusion

1. The algorithm and program realization to quantify the effects of impacts on the automated system of internal and external dependent threats, not previously used by researchers to obtain a quantitative assessment of information security of restricted access.

2. Results of mathematical modelling can be characterized as new scientific results in practice data protection will allow owners of restricted information to develop science-based activities for the protection of information resources, circulating in computer systems and networks.

3. The results of this work indicate the need to strengthen the researchers on the development of new techniques and methodologies for evaluating security of information with restricted access, because this helps to significantly affect the protection available to the owner of the information resources, reduce risks and losses from the sale of the attacker limited access information security threats.

References

[Ros10] Rosenko, A.P. 2010, "Internal threats to the security of confidential information: methodology and theoretical research", Monograph, pp. 160.

[Hus13] Huseynov, S.T. 2013, "Methodology of laboratory workshops on computer modeling with programming in Microsoft Excel Visual Basic for applications", AICT 2013 - 7th International Conference on Application of Information and Communication Technologies, Conference Proceedings.

[Lei13] Leite, M.D., Marczal, D. Pimentel, A.R. 2013, "Multiple external representations in remediation of math errors", ICEIS 2013 - Proceedings of the 15th International Conference on Enterprise Information Systems, pp. 519.

[Yan13] Yang, D. 2013, Empirical analysis of the demand for interpretation system of world cultural heritage based on optimized selection model and mathematical physics equations.

[Zyr16] Zyryanov, Y.U. 2016, "Informatsionnaya bezopasnost ERP-sistem" (URL: http://citforum.ru/gazeta/49/)

[OEC16] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 2016. (URL: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf)

[Sch11] Schjolberg S., Ghernaouti-Hlie S. 2011, "A Global Treaty on Cybersecurity and Cybercrime", Second edition. (URL: http://www.cybercrimelaw.net/documents/)

[Sum12] Summary of responses to the survey on the implementation of the OECD guidelines for the security of information systems and networks: towards a culture of security 2012. (URL: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8 /FINAL&docLanguage=En)

[OEC12] OECD Cybersecurity policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet Economy. (URL: http://www.oecd.org/officialdocuments/)

[OEC15] OECD Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI. (http://dx.doi.org/10.1787/9789264245471-en)

[Kor14] Korshunova, O.N., Razumovskaya, E.A. 2014, "Some information security problems", pp. 83–91.

[Cer13] CERT Insider Threat Team. Unintentional Insider Threats: A Foundational Study. – Carnegie-Mellon University. Software Engineering Institute, CERT Division. – Pittsburg., 2013. – 91 .

[IBM13] IBM SPSS Modeler 16 Algorithms Guide 2013. (URL: http://public.dhe.ibm.com/software/analytics /spss/documentation/modeler/16.0/en/ AlgorithmsGuide.pdf)