Development of Methods and Software Modules Security Assessment Information of Limited Distribution

Tebueva F.B.
NCFU
Stavropol
fariza.teb@gmail.com

Rosenko A.P.
NCFU
Stavropol
Rap.44@mail.ru

Nechvoloda V.E.
NCFU
Stavropol
nechvolodaa@yandex.ru

Smykova V.N.
NCFU
Stavropol
zwho27@yandex.ru

Abstract

This article leads a research on the development of a method and a program module evaluating the security of information of restricted access (IRA). The assessment of existing security technologies for information of limited access is given. Based on the general method of quantitative assessment of the safety of IRA a private method of quantitative assessment of the safety of IRA has been developed for a continuous flow of threats. The algorithm of the program for assessing the security of restricted access information for a continuous flow of threats has been developed and described.

Keywords: safety assessment, information is restricted, mathematical modeling, the probability of a successful outcome, the intensity parry threats to the flow rate, security technology, security assessment, restricted access information, probability of successful outcome, parry intensity, intensity of threat flow, security technology.

1 Introduction

The protection of information of limited access (IOD) is one of the main tasks facing the legal owner of information. At present, the issues of protecting IOD in the enterprise are very relevant [1, 2, 3, 4]. Almost every organization operates in its systems IOD, or is a processor of personal data of its employees.

There are various methods for assessing the security of IOD. One way to protect IOD is to develop and apply mathematical models to study the effect of threats on IOD security.

The most preferred are mathematical models based on Markov random processes.

In: S. Hölldobler, A. Malikov (eds.): Proceedings of the YSIP-3 Workshop, Stavropol and Arkhyz, Russian Federation, 17-09-2019–20-09-2019, published at http://ceur-ws.org

Information technologies include methods for collecting information, its processing, transformation, storage and distribution [1, 2, 3, 4, 5].

The formation of the process of electronic information space is accompanied by the development of methods for ensuring the protection of information circulating in it. So an organization that cares about the protection of restricted access information (IOD) circulating in it, has to implement a whole range of measures to ensure the security of information. The following groups are most pressing problems in the field of computer security for IRA [2, 5, 6]:IRA integrity violation, IRA confidentiality violation, violation of automatic information systems (AIS) that processes IRA: IRA integrity violation, IRA confidentiality violation, violation of automatic information systems (AIS) that processes IRA.

One of the directions of scientific research of confidential information security is a natural experiment.The method is based on the fact that at the preparatory stage an absolute copy of the protected information system is created, all interrelations between the system objects (internal and external) are established. Then all sorts of attacking actions of intruders begin to be modeled in order to overcome the organizations security system. The result is statistical data on the modelling.

There are two strategies for natural experiment: active and passive. In the first case the experimenter has the ability to change the external conditions that determine the state of the object. Second - this is not possible. The advantage of this method the high accuracy of the results of the experiment. The main disadvantage of such research are the complexity and high cost of experimental studies, as is required to put into practice a large number of identical experiments.

Another method to study the safety of restricted information is semi-natural modeling.Semi-natural modeling is a kind of experimental theoretical study in which several nodes investigated system is replaced by their physical counterparts [2]. The method allows the study not to create a complete copy of the studied information system. Due to the fact that some assumptions were made, respectively decreases the accuracy of the study, the error appears. Also, another disadvantage of this method is that the established experimental model will not be enough similar to the real system that was introduced in full-scale experiment, thereby decreasing reliability. However, because of the insufficient development of the mathematical apparatus, an excessively large dimension of the problem, the large number of random factors, this method is often not applicable [2].

To solve the problem of analyzing a security system containing IRA, it is proposed to use a mathematical modeling apparatus based on Markov random processes. This mathematical model has all the functionality necessary to simulate the security of a system against accidental and deliberate threats. However, there are many other methods by which it is possible to analyze the security of information of various in-formation systems. So, in the article [7, 8] for network security and traffic estimation the tensor method is used, providing scalable data analysis and reducing the cognitive load of network analysts. Since the events occurring in networks and information systems are random, then Markov random processes are the most suitable for studying them. The source [9] presents a structure for modeling and assessing IoT security, which consists of five stages: data processing, generation of a security model, security visualization, security analysis and model updates. This technique allows to find possible scenarios of attacks on IoT, determine the most vulnerable part of the network, evaluate the effectiveness of various protection mechanisms and choose the method that is optimally suitable for solving emerging problems. The study [10] describes the method of stochastic security assessment, which is based on the model of attack protection trees to represent security scenarios. This method can be supplemented with the use of a mathematical model of Markov random processes, the structure and features of which are analyzed in this paper. In the source [10], an algorithm was proposed for searching and making optimal management decisions to reduce the current risk values to the target level. The introduced metrics make it possible to quantify how dangerous the current situation is, as well as to compare the situations with each other. The article [11] assesses the reliability parameters of a secure payment system in e-commerce, where the analysis of existing systems showed that information security was possible in them if the core of the integrated protection system contains firewall technology built on distributed attack detection methods. Thus, the purpose of this article is to develop a method and software module for assessing the security of information of limited distribution based on Markov random processes

2 Methods

2.1 Formulation of the problem

The impact of accidental threats to the security elements of IRA system can result in two outcomes [1, 12, 7]:

1. A favorable outcome - a random threat did not materialize, which means that the taken measures were enough for random threat parry.

2. Not a favorable outcome - the taken measures were not enough for random threat parry.

As a result, it is proposed as a criterion for quantifying IRA security, likely to take a successful outcome from exposure to threats random system. This probability is de-noted by p, and the probability of the opposite event is denoted by q. Since the magnitude of the favorable and unfavorable outcome constitute a complete group of events, then the condition [1, 12, 7]:

$$p + q = 1 \tag{1}$$

The probability of the i-this a special situation q_i, and the conditional probability of it reflect the effects of its occurrence r_i, and the probability of not reflect the effects of $\overline{r_i}$.

Then we define the probability q_i and p_iAs automatic information system (AIS) sequence of transitions from one state to another in a Markov random process with a number of states and continuous time. This process is conveniently represented as a logical - probabilistic process. [1, 9, 10].

Fig. 1 shows that there is a threat of IRA exposure to security threats in the AIS. At this time, the system state may be described by the following conditions [1, 9]:

- ¡¡O¿¿ – the initial state of the AIS;
- ¡¡$\overline{\text{BY}}$¿¿ – a condition in which i – th threat was not realized with the probability p_i;
- ¡¡BY¿¿ – a condition in which i – th threat manifested itself with probability q_i;
- ¡¡P¿¿ – a condition in which i-th threat is countered by protection system with probability r_i;
- ¡¡$\overline{\text{P}}$¿¿ – a condition in which i-th threat is not countered by protection system with probability r_i.

State ¡¡BY¿¿ and ¡¡P¿¿ are states of a successful outcome when exposed to AIS security risks of IRA and is expressed by formula [1, 12, 9, 10, 7]:

$$P_{\text{bi}_i} = p_i + q_i r_i \tag{2}$$

State ¡¡$\overline{\text{P}}$¿¿ is a condition characterized by the occurrence of an event unfavorable outcome, when IRA exposed to security threats and expressed by the formula:

$$Q_{\text{bi}_i} = q_i \overline{r_i} \tag{3}$$

Likelihood Q_{bu_i} andP_{bu_i}form a complete group of events, and thus fulfilled the formula:

$$Q_{\text{bi}_i} + P_{\text{bi}_i} = 1 \tag{4}$$

Affecting AIS IRA security threats can be generated by a one with a certain probability. It is therefore proposed to adopt a base - model of Markov processes with continuous parameter for safety assessment, taking into account the impact on AIS dependent flows threats. The process of mathematical modeling of complex systems based on a Markov random process can be divided into three successive steps - building a mathematical model, developing and modeling an algorithm for building a model based on Markov processes, studying the original system with a model that represents an experiment, processing and interpreting the results.

2.2 Development and research of the method of the software module for quantitative assessment of the security of restricted access information

In Markov processes AIS future state depends on the last only through the present.

A random process with respect to the AIS is called Markov if for any time t_0 probability of AIS in the future depends only on its state at the moment t_0 and does not depend on when and how AIS came into this state [1, 4, 5].

Classification of Markov random process is performed depending on the continuous or discrete values of the set function X (t) and the parameter t [13, 14].

Let AIS on a finite time τ acts n just a stream of threats with intensities λ_i. i= 1,n.

Let μ_i– the intensity of the effects Parry i-the second threat. Respectively,R_i– parry, and $\hat{R}_i$– the probability of not parry i-th threat.

Then, $\mu_i \cdot R_i$– the intensity of the parry and $\mu_i \cdot \hat{R}_i$– the intensity is not parry impacts on the flow of AIS threats.

Assumptions: parry flow and not parry the threat of the simplest, ability to parry the effects of exposure to AIS i– second threat is not limited, that is, $\mu_i \geq \lambda_i$, since these elementary streams, the appearance at the same time two or more threats is impossible event.

To determine the probability of a successful outcome when exposed to the flow of AIS n threats the AIS system is represent as a graph.

Referring to figure 1, the AIS at time τ may be in one of the following conditions [1, 4, 6]:

- state ¡¡0¿¿– the flow of threats over time τ failed to appear;
- state ¡¡1¿¿, i..., n– one of the threats was manifested;
- state ¡¡n+1¿¿ – unfavorable absorbing state in which the threat was realized.

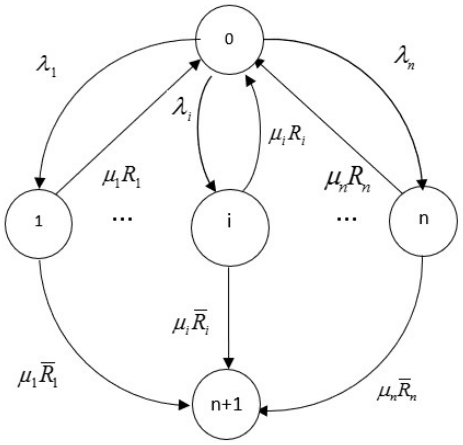

Figure 1: Graph AIS states when exposed to n independent streams threats

According to figure 1 can write intensities transition matrix form:

$$\|\lambda_{jk}\| = \begin{vmatrix} -\lambda_0 & \dots & \lambda_i & \dots & \lambda_n & 0 \\ u_i R_i & \dots & -u_i & \dots & 0 & u_i R_i \\ u_n R_n & \dots & 0 & \dots & -u_n & u_n \overline{R_n} \\ 0 & \dots & 0 & \dots & 0 & 0 \end{vmatrix}, \quad (5)$$

where$\lambda_0 = \lambda_1 + \lambda_2 + \ldots + \lambda_n,\ j = k = 1, 2, \ldots, n+2.$

Matrix (5) has the following properties:

- the diagonal terms of the matrix are equal to the sum of the remaining elements of the line, taken with the opposite sign;

- the sum of all elements in each row is equal to zero;
- the number of zero crossings in the matrix rows correspond to the number of intensities absorbing states;
- the transition intensity is zero in the absence of the arrow.

To determine the AIS transition probabilities to each possible state of the system Kolmogorov differential equations are used, in accordance with which one can write:

$$\frac{dP_0(\tau)}{d\tau} = -P_0(\tau)\sum_{i=1}^{n}\lambda_i + \sum_{i=1}^{n}\mu_i R_i P_i(\tau) \frac{dP_i(\tau)}{d\tau} = \lambda_i P_0(\tau) - \mu_i P_i(\tau) \frac{dP_{n+1}(\tau)}{d\tau} = \sum_{i=1}^{n}\mu_i \hat{R}_i P_i(\tau) \tag{6}$$

Applying to the set of differential equations (6) the direct the Laplace transform to the reference data $P_0\,(0) = 1.\ P_i\,(0) = \mathrm{P_{n+1}}\,(0) = 0$ and given the fact that $\int_0^\infty P\,(\tau)\,e^{-\mathrm{S}t}\mathrm{d}t = -\,P_i\,(0) + \mathrm{SP}_j\,(S)$, the following expression for determining probabilities in accordance with the count states is obtained (figure 1).

$$\begin{aligned} -P_0(0) + SP_0(S) &= -\lambda_0 P_0(S) + \sum_{i=1}^{n}\mu_i R_i P_i(S) \\ -P_i(0) + SP_i(S) &= \lambda_i P_0(S) - \mu_i P_i(S), \\ -P_{n+1}(0) + SP_{n+1}(S) &= \sum_{i=1}^{n}\mu_i \hat{R}_i(S) \end{aligned} \tag{7}$$

where$P_i\,(S) = \int_0^\infty P_i\,(\tau)e^{-St}d\tau$– the desired image.
For the initial conditions of equations (7) becomes:

$$(S+\lambda_0)P_0(S) = \sum_{i=1}^{n}\mu_i R_i(S) = 1 - \lambda_i P_0(S) + (S+\mu_i)P_i(S) = 0 - \sum_{i=1}^{n}\mu_i \hat{R}_i P_i(S) + SP_{n+1}(S) = 0 \tag{8}$$

According to Cramer's rule the desired image is determined by the ratio:

$$P_j(S) = \frac{\Delta_j(S)}{\Delta(S)}, j = 1, n \tag{9}$$

where$\Delta(S) = S[(S+\lambda_0)\prod_{i=1}^{n}(S+\mu_i) - \sum_{i=1}^{n}\lambda_i\mu_i R_i \prod_{i=1}^{n} S+\mu_l)]$ – the main determinant of the system; $\Delta_j(S)$ – partial determinant system, is the main determinant by replacing j-th column coefficients on the right of equations (8). [13, 12].

Private determinants obtained by introducing determinants of induction will be equal to:

$$\Delta_0(S) = S\prod_{i=1}^{n}(S+\mu_l) \tag{10}$$

In view of the indicated and with the proviso that $\rho_j(S) = \frac{\Delta_j(S)}{S}$, $\rho(S) = \frac{\Delta(S)}{S}$the system of equations (8) takes the form:

$$\begin{aligned} P_0(S) &= \frac{q_0(S)}{\rho(S)} = \frac{\Delta_0(S)S}{S\Delta(S)} = \frac{\Delta_0(S)}{\Delta(S)} \\ P_i(S) &= \frac{q_i(S)}{\rho(S)} = \frac{\Delta_i(S)S}{S\Delta(S)} = \frac{\Delta_i(S)}{\Delta(S)} \\ P_{n+1}(S) &= \frac{q_{n+1}(S)}{\rho(S)} = \frac{\Delta_{n+1}(S)S}{S\Delta(S)} = \frac{\Delta_{n+1}(S)}{\Delta(S)} \end{aligned} \tag{11}$$

Finally, with regard to (10) the expressions (11) take the form:

$$\begin{aligned} P_0(S) &= \frac{q_0(S)}{\rho(S)} = \frac{\Delta_0(S)S}{S\Delta(S)} = \frac{\Delta_0(S)}{\Delta(S)} \\ P_i(S) &= \frac{q_i(S)}{\rho(S)} = \frac{\Delta_i(S)S}{S\Delta(S)} = \frac{\Delta_i(S)}{\Delta(S)} \\ P_{n+1}(S) &= \frac{q_{n+1}(S)}{\rho(S)} = \frac{\Delta_{n+1}(S)S}{S\Delta(S)} = \frac{\Delta_{n+1}(S)}{\Delta(S)} \end{aligned} \tag{12}$$

Then the probability of a successful outcome of the impact on AIS n independent internal threats streams determined by the following expression:

$$P_{\text{bi}}(\tau) = \sum_{i=1}^{n} P_i(\tau) \tag{13}$$

The probability of the opposite event, ie, an unfavorable outcome will be equal:

$$P_{\text{bb}}(\tau) = 1 - \sum_{i=1}^{n} P_i(\tau) = P_{n+1}(\tau) \tag{14}$$

For practical purposes it often occurs that the AIS is affected by one stream of threats, ie n =1.

It is supposed that the AIS, in the course of time τ is affected by one stream of threats to the intensity – λ Intensity of Parry - μ and parry threats flow probability –R[15, 9].

Then the system of equations (12) n =1 Probability image will look like this:

$$\begin{aligned} P_0(S) &= \frac{S+\mu}{(S+\lambda)(S+\mu) - \lambda\mu R} = \frac{q_0(S)}{\rho(S)} \\ P_1(S) &= \frac{\lambda}{(S+\lambda)(S+\mu) - \lambda\mu R} = \frac{q_1(S)}{\rho(S)} \\ P_{n+1}(S) &= \frac{\lambda\mu\hat{R}}{S[(S+\lambda)(S+\mu) - \lambda\mu R]} = \frac{q_{n+1}(S)}{S\rho(S)} \end{aligned} \tag{15}$$

where$\rho(S) = S^2 + Sc_1 + c_0$, $\mathrm{c}_1 = \lambda + \mu$, $\mathrm{c}_0 = \lambda\mu\hat{R}$.

Applying to the (15) the inverse Laplace transform of taking (13) and (14) the expression for the determination of the desired probability is obtained, namely:

$$P_0(\tau) \to P_0(\tau) = \frac{1}{2\sqrt{\Lambda}} e^{-\frac{c_1}{2}\tau}[(\mu - \lambda - \Lambda)e^{-\frac{\sqrt{\Lambda}}{2}\tau} - (\mu - \lambda - \sqrt{\Lambda}e^{-\frac{\sqrt{\Lambda}}{2}\tau})] \tag{16}$$

$$P_0(\tau) \to P_0(\tau) = \frac{1}{2\sqrt{\Lambda}} e^{-\frac{c_1}{2}\tau}[(\mu - \lambda - \Lambda)e^{-\frac{\sqrt{\Lambda}}{2}\tau} - (\mu - \lambda - \sqrt{\Lambda}e^{-\frac{\sqrt{\Lambda}}{2}\tau})] \tag{17}$$

$$P_{n+1}(\tau) = 1 - \frac{2\lambda\mu\hat{R}}{\sqrt{\Lambda}} e^{-\frac{c_1}{2}\tau}[\frac{1}{\lambda + \mu - \sqrt{\Lambda}} e^{-\frac{\sqrt{\Lambda}}{2}\tau} - \frac{1}{\lambda + \mu + \sqrt{\Lambda}} e^{-\frac{\sqrt{\Lambda}}{2}\tau})] \tag{18}$$

where $\Lambda = c_1^2 - 4c_0 = \lambda^2 + 2\lambda\mu(1 - 2\hat{R}) + \mu^2$.

Then, taking into account (13) and (14) the probability of a successful outcome from the effects of AIS threats will be equal to:

$$P_{\text{bi}}(\tau) = P_0(\tau) + P_1(\tau) \tag{19}$$

and the probability of an unfavorable outcome:

$$Q_{\text{BI}}(\tau) = P_{n+1}(\tau) \tag{20}$$

2.3 Development of a IRA software security assessment module

Based on the method of evaluation of information security limited access, for one continuous flow threats examined input parameters to the algorithm, and the output parameters that the algorithm, which block diagram is shown in Figure 2 must provide the program on the basis of the work, it has been realized.

To implement the safety assessment algorithm IRA was selected Java SE 8, a programming language, because it provides more opportunities for programming Windows and Linux operating system applications. For the development was chosen IntelliJ IDEA development environment that includes a high-performance tool visually build applications based on GUI programming library Swing and AWT [11, 10, 16].

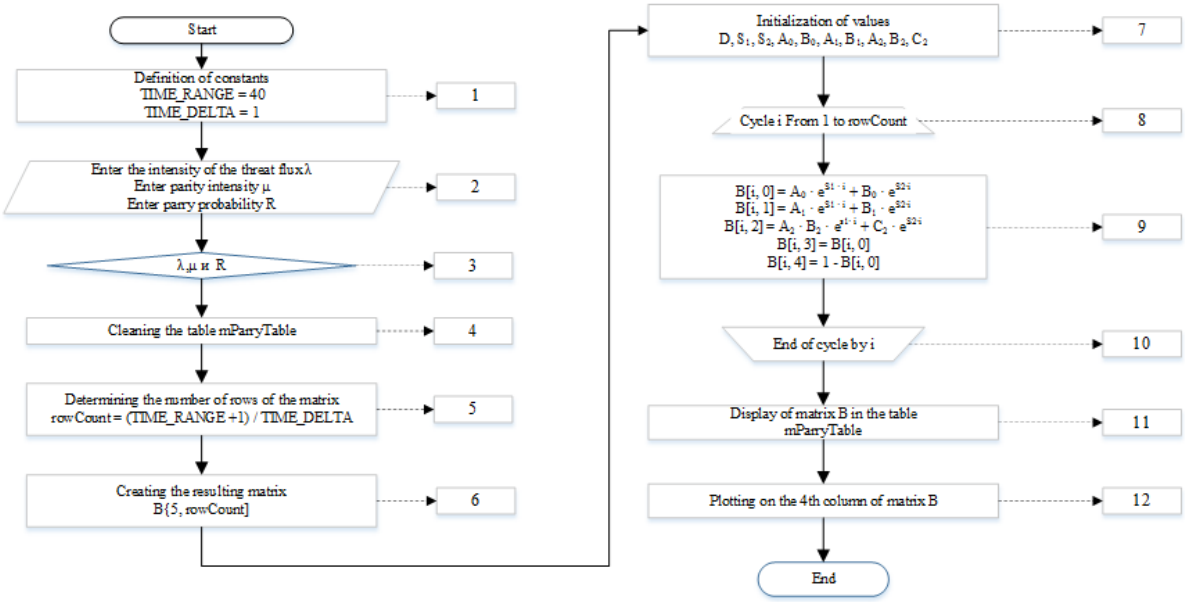

Figure 2: A block diagram of the algorithm

The algorithm of the IOD safety assessment program is developed on the basis of the flowchart of the method for quantifying the safety of IOD for one continuous flow of threats, presented in the flowchart in Figure 2.

As seen from the block diagram in the block number 1 initialization constants necessary for further operation of the algorithm is carried. Namely TIME_RANGE constant is set to 40, which determines the exposure time on stream AIS threats, TIME_DELTA to 1, which corresponds to the time sampling rate threats stream impacts on the system.

The block number 2 is the input of the input data: the flow rate of threats λ, the intensity parry threats μ, parry R.

In block number 3 input valid data-in is checked, if the data is correct, then control is passed to the block number 4, otherwise, control is transferred to block number 2, to re-enter the input data.

The number 4 unit is cleaned mParryTable component fields of data that it can contain the above [6, 15].

A variable rowCount (rowCount = (TIME_RANGE + 1) / TIME_DELTA) is determined in the room unit 5 the number of rows of the matrix to be created at step 6.

The resulting empty matrix B, comprising 5 rowCount columns and rows is created in room unit 6.

The auxiliary values are initializes the room unit 7:

$$D = \mu^2 + \lambda^2 + 2 * \lambda * \mu * (2 * R - 1);$$
$$s_1 = -\frac{\left(\mu + \lambda + \sqrt{D}\right)}{2}; \quad s_2 = -\frac{\left(\mu + \lambda - \sqrt{D}\right)}{2}$$
$$B_0 = \frac{\mu + s_2}{s_2 - s_1};\ A_0 = 1 - B_0;\ B_1 = \frac{\lambda}{s_2 - s_1};\ A_1 = -B_1; \tag{21}$$

$$A_2 = \frac{\lambda * \mu * (1 - R)}{s_1 * s_2};\ C_2 = -\frac{s_1 * A_2}{s_1 - s_2};\ B_2 = -A_2 + C_2.$$

In the 8-block is generated by a variable cycle i, sequentially taking values from 0 to rowCount.

In block number 9, the values of matrix B are assigned in accordance with step i. B [i, 0] - the probability of the system in state 0, B [i, 1] - in state 1, B [i, 2] - in state 2, B [i, 3] - the probability of a successful outcome, B [i, 4] - the probability of an unsuccessful outcome. To calculate the probabilities, the values obtained in block 7 of algorithm (21) are used, as well as the following formulas:

$$\begin{gathered} B[i,0] = A_0 * e^{s_1 * i} + B_0 * e^{s_2 * i}; B[i,1] = A_1 * e^{s_1 * i} + B_1 * e^{s_2 * i}; \\ B[i,2] = A_2 + B_2 * e^{s_1 * i} + C_2 * e^{s_2 * i}; \\ B[i,3] = B[i,0]; B[i,4] = 1 - B[i,0]. \end{gathered} \tag{22}$$

In block 10, the boundary of the cycle in the variable i is implemented.

In block 11, the values of the matrix B are mapped to the mParryTable component.

In block 12, a graph is constructed on the 4th column of matrix B.

Let us conduct a modelling of a quantitative assessment of the security of the IOD, to study the influence of the time parameter of the impact of the threat flow on the AIS on the probability of a successful outcome [4, 17, 13]. Input data for the simulation are shown in table 1.

Table 1: Input parameters

The intensity of the threats flow	1
The intensity parry	1
Parry probability	0,8

3 Results

As a result of the program, statistics were obtained that are presented on the graph of the dependence of a successful outcome on the time of the impact of the threat flow in Figure 3.

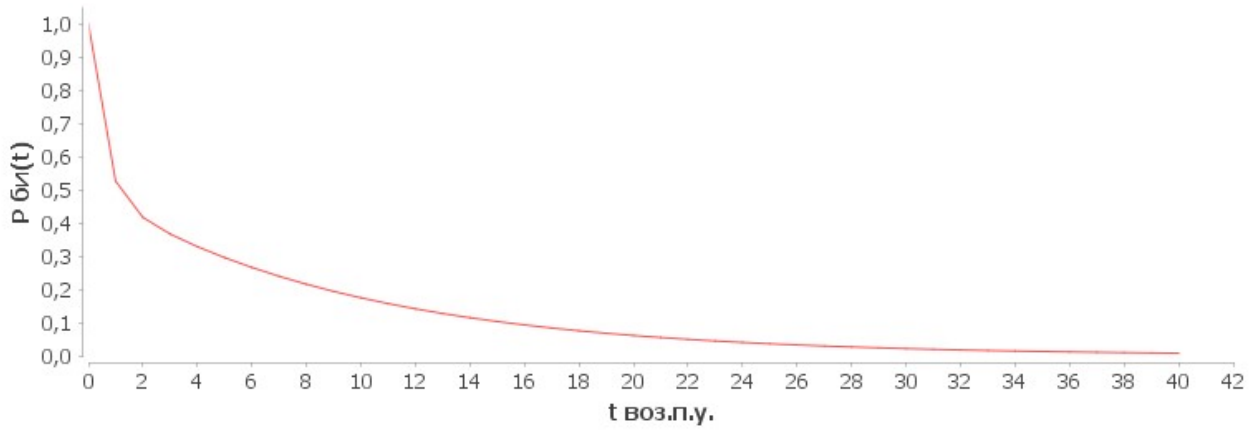

Figure 3: Graph of successful outcome P_{bi} of exposure time threats flow

The graph shown in figure 3 can observe the probability of a successful outcome decrease with increasing exposure time on stream AIS threats [3, 18, 14].

As a result, conclusions can be drawn: probability P_{bi} of AIS successful outcome from exposure to the flux IRA threats decreases with increasing exposure time threats stream, the rate of decrease in probability P_{bi} depends on the probability of countering the threat, as well as on the intensity of the impact of the flow of threats.

Let us conduct a modelling of a quantitative assessment of the security of the IOD, to study the influence of the parameters of the intensity of the threat flow and the intensity of the parry, on the probability of a successful outcome. To do this, several different sets of input parameters, with different indicators of the intensity of the threat flow and the intensity of the parry, and a fixed value of the probability of parry.

The value of the probability of parrying by setting the value to 0.6 is fixed. The values of the intensity of the flow of threats and the intensity of parry together, from a value of 0.1 to 3 are changed.

Based on the modelling, a graph of the overall modelling results for various intensities of the threat flow and the intensity of parry is built, the results are presented in Figure 4.

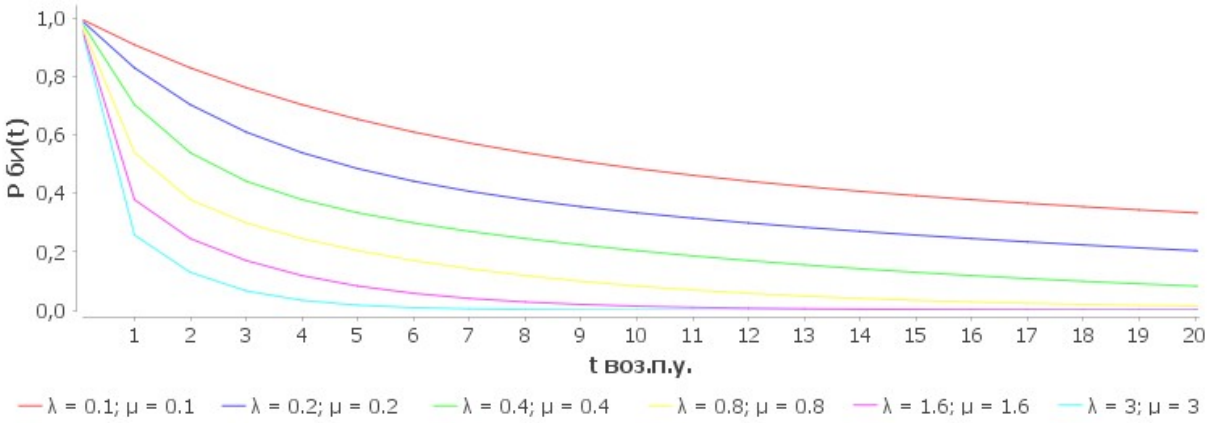

Figure 4: Graph of successful outcome P_{bu} of exposure time threats stream at different intensities and intensity threats parry flow

Based on Figure 4, it is concluded: the probability of a successful outcome for AIS, from the impact of the flow of threats from the IOD on it, depends on the intensity of the flow of threats and the intensity of parry. The greater the intensity of the threat flow and the intensity of the parry, the faster it decreases, which means that AIS prone to a more intense flow of threats is less secure.

4 Discussion

As a method and software module for assessing the security of information of limited distribution, a mathematical modeling apparatus based on Markov random processes was analyzed. This mathematical model has all the functionality necessary to simulate the security of a system against accidental and deliberate threats. Its use will allow to accurately determine the flow of the impact of threats on the AIS.

5 Conclusion

The aim of this study was to increase the security of AIS using the method developed information security assessment of restricted access and its software implementation. To achieve this, all the tasks were performed.

In the process, an analysis of existing security restricted information technology, concluded the relevance assessment IRA security.

In the next step the existing methods of assessing the safety of restricted information were studied, namely: a natural experiment, simulation and semi-natural method of expert evaluations. The method of mathematical modeling based on Markov processes was proposed.

A general method of information security assessment on the basis of the limited access of Markov is processed. Based on the general method for quantifying the safety of IOD, a particular method has been developed for quantifying the safety of IOD for a continuous flow of threats. A software module was developed.

References

[1] M. M. Baskaran et al. “Enhancing network visibility and security through tensor analysis”. In: *Future Generation Computer Systems* (2019).

[2] Karim Lounis. “Stochastic-based Semantics of Attack-defense Trees for Security Assessment”. In: *Electronic Notes in Theoretical Computer Science 337* (2018).

[3] M. Ge et al. “A framework for automating security analysis of the internet of things”. In: *Journal of Network and Computer Applications* (2017).

[4] D. Lovtsov, D. Makarenko, and A. Fedichev. “Architecture of the national classification of legal regimes of restricted access information”. In: *CEUR Workshop Proceedings* (2017).

[5] A. P. Rosenko and E. A. Nekrasova. “Mathematical modelling of the process for impact on automated information system security of threats access to restricted information”. In: *CEUR Workshop Proceedings* (2017).

[6] Vybornova O. N. Azhmukhamedov I.M. “Introduction of metric characteristics for solving the problem of risk assessment and management”. In: *Caspian Journal: Management and High Technologies* (2015).

[7] Barry K. Schwartz. “Overview of security technology efforts at Bell Communications Research”. In: (1989).

[8] J. M. P. Ramirez. “Limits on transparency. Scope of the restricted right of citizens to access to information held by the European institutions [Los li´mites a la transparencia. El menguado alcance del derecho de los ciudadanos a acceder a la informacio´n en poder de las instituciones Europeas]”. In: *Teoria y Realidad Constitucional* (2014).

[9] D. Gabbay and A. Hunter. “Restricted access logics for inconsistent information”. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (1993).

[10] S. Budiansky. “Us Nuclear Information: Opposition To Proposals For Restricted Access”. In: *Nature* (1993).

[11] Y. Zheng. “A study on network security technology based on Web Service”. In: *2011 International Conference on Computer Science and Service System* (2011).

[12] Strokacheva O. A. Tishchenko E.N. “Evaluation of the reliability parameters of a secure payment system in electronic commerce”. In: *Bulletin of the Rostov State Economic University (Rinh)* (2006).

[13] E. M. Meyers. “Access denied: How students resolve information needs when an ”ideal” document is restricted”. In: *ACM International Conference Proceeding Series* (2012).

[14] C. Wang, Z. Zhang, and X. Song. “Research on the information security technology of university campus network”. In: *Advances in Intelligent and Soft Computing, AISC (VOL. 2)* (2012).

[15] H. Wang et al. “The security protection and technology analysis of information system”. In: *Applied Mechanics and Materials* (2013).

[16] C. Tang. “Study of security technology in wireless sensor networks”. In: *Lecture Notes in Electrical Engineering, 219 LNEE (VOL. 4)* (2013).

[17] F. Li. “Research on database security technology”. In: *Lecture Notes in Electrical Engineering, 138 LNEE* (2013).

[18] G. A. Suer, A. Arynsoy, and O. Ates. “Bi-objective family scheduling problem with fuzzy math modeling”. In: *IIE Annual Conference and Expo* (2013).