A mathematical model for assessing security of restricted-access information

A P Rosenko, V I Petrenko, F B Tebueva and A A Gerasimova
North Caucasus Federal University, Pushkin street, 1, Stavropol, 355009, Russia

E-mail: fariza.teb@gmail.com

Abstract. An immediate problem of the theory on information security lies in measuring security of restricted-access information. The existing methods are not capable to solve the above problem due to lack of a priori background information. The paper is aimed at filling the gap created in the theory on assessing RAI security using quantitative approach.

1. Introduction

The provision of restricted-access information (RAI) security has always been and remains one of the most important problems faced when protecting information (IP) [1-3]. Not only RAI owner, but also a state as a whole suffers considerable material and moral damages from RAI leakage. This is because there are obvious and quite objective laws emergent in the present-day challenging conditions of information relationship. Contemporary information technologies widely used to process RAI create a major source of threats to information security (IS), since, simultaneously, methods and means for acquiring unauthorized data are significantly evolving. The above conditions resulted in a situation where a threat to RAI from certain law-breakers and organized criminal associations can be compared to a threat to information from foreign technical intelligence services [4-6].

Analyzing the current state of RAI security testifies that multiple and mostly hidden relationships between certain components of AIS as a complex dynamic system are specified by actions of men and other internal and external factors effecting, for instance, the level of RAI security. Thus, scientific and methodological frameworks for ensuring RAI security need to be developed and implemented in action [2,6].

Nowadays, due to a number of objective primarily economic reasons, a situation is brought about when theoretical developments and applied IP methods and means are mostly aimed at obtaining quality parameters. The problem becomes more compounded due to a priori lack of the initial information that restricts use of assessing RAI security using quantitative approaches that, in its turn, makes RAI security theory lag behind the level of IP theory development.

RAI security is a major parameter that implies a security level of AIS and its relatively autonomous structural elements, whereby protection of RAI is assured with a required degree of probability from leakage, theft, loss, erasure, distortion, copying, blocking. It is known that RAI security is provided throughout the whole period of its lifetime. However, as far as confidentiality compliance is concerned, the most important stage involves using RAI as intended. Studies show that it is precisely at this stage maximum unauthorized activities are observed. At the same time, analysis of statistical data reveals that most cases of unauthorized access to RAI arise due to so called anthropogenic factors that, in its turn, depend on men’s activity or inactivity resulting in intentional or unintentional mistakes of both an owner,
and users of RAI. It is caused by a failure to observe the rules of RAI handling, inadequate level of knowledge, skills, and practical skills on using the existing IP means and methods. All the above-stated is indicative of a necessity for treating AIS as a complex man-machine system with attributes inherent to the complex systems [3, 6, 7].

At the same time, as analysis shows, the problem of assessing RAI security through quantitative approach is exacerbated by the following objective and subjective reasons:

• utilized methods, means, and measures aimed at protecting RAI are qualitative that doesn’t facilitate establishment of scientifically-proven cause and effect relationships formed in AIS under effect of various threats;
• there is a substantial non-conformance between realizing a need for assuring RAI security and implementation of the existing methods and means used to protect it, between serious danger of different threats and means taken to prevent them;
• non-conformance between obvious importance of the problem and paces of pioneering fundamentally new prospective IP methods and means aimed at preventing unauthorized access to RAI based on mathematical and computer modelling methods.

Thus, the analysis reveals that there are inconsistencies in RAI security theory and practice as follows:

• between the need for measuring RAI security and lack of methodological and theoretical tools for such assessment bearing in mind threats of various types that affect AIS;
• between necessity of obtaining and assessing authentic information on consequences resulting from impact of various threats on AIS and limited capacities of the existing methods and methodologies in terms of the number of the parameters assessed and potential AIS states.

The said inconsistencies shall, within this manuscript, create the following objective of the study: theoretical generalization, development of mathematical model and mathematical modelling to solve problems of assessment using quantitative approach and predicting RAI security taking into account impact of inside and outside threats on AIS.

For the purposes of this study, a probability of successful (unsuccessful) outcome of law-breaker’s carrying out inside and outside threats is assumed to be a criterion for assessing RAI security.

To achieve the objective formulated, the following problems raised in the study need to be addressed:

• analysis of the current state and directions of developing methodological and theoretical backgrounds of analyzing and synthesizing RAI security;
• development of criteria for assessing and predicting RAI security taking into account impact of inside and outside threats on AIS;
• development of numerical method and mathematical model, and software implementation to measure consequences resulting from impact of RAI security threats on AIS based on Markov random processes with discrete states;
• mathematical modelling and undertaking study of RAI security taking into account impact of various threats on AIS; development of scientifically proven practical recommendations aimed at assuring RAI security.

It should be stressed that Russian and foreign scientists [1-15] made a huge contribution to shaping new attitudes towards the problem importance, created a need for developing and introducing brand-new scientifically proven means, methods, and technologies. Thus, authors, in their works, are investigating fundamental problems of IP and IS theory and practice for developing common
methodological approaches, methods, and methodologies of assessing and analyzing the state of the problem, reaching the most optimal solutions to the first-priority problems in the area in question.

Obviously, use of the results of the above studies for practical purposes facilitates improvement of securing the information that circulates in local and corporate networks, and information in hard copies. However, analysis of applying IP methods and means shows that the rates of their development and introduction remain short of the primary needs prescribed by the tendencies of developing means and methods of unauthorized access to RAI.

An obvious fact should be noted based on the results of the above analysis that there is no enough attention paid to the problem of studying impact of human factor on RAI security, and, thus, developing methods and countermeasures against various threats. In this regard, works made under the guidance of Kostogryzov A.I., Prof., Dr. of Engineering Science, are worthy of most interest. A simulation complex of tools is created under his guidance to assess quality of information system performance that enables to obtain, through modelling the processes of operation of real information systems, probabilities of achieving objectives of such systems, compare danger of particular threats and assess efficiency of using appropriate information technologies. Here, of special attention is the security of information bearing in mind men’s activities.

However, it should be mentioned that a problem of measuring RAI security is not properly handled, since, first and foremost, this problem relates to solving weakly formalizable task, i.e. it is challenging to have a mathematical description of a man-machine information system. This paper offers a possibility of measuring RAI security through Markov random processes used for AIS.

2. Materials and methods

2.1. System state graph

Let there be \( n \) dependent threats effecting AIS that may be cross-generated with probabilities \( r_1, \ldots, r_n \). Such process may be presented as a state graph as it is shown in figure 1 [13].

Let’s assume the following notations:

- \( q_0, q_1, \ldots, q_n \) – probabilities of \( i^{th} \) threat occurrence;
- \( R_0, R_1, \ldots, R_n \) – probabilities of correcting \( i^{th} \) threat occurred;
- \( \bar{R}_0, \bar{R}_1, \ldots, \bar{R}_n \) – probabilities of failure to correct \( i^{th} \) threat occurred;
- \( 0, 1, \ldots, n, n + 1 \) – possible states of the system in question as a result of \( n \) dependent threats’ effecting it. Then, state \( n + 1 \) corresponds to absorbing state. Absorbing state characterizes law-breaker’s carrying out \( i^{th} \) threat.

![Figure 1. State graph when \( n \) dependent threats effect a system.](image-url)
As per figure 1, matrix of probabilities of system transition from one state to the other may be presented as follows:

\[
\begin{pmatrix}
1 - q_x & q_{ii} & \ldots & q_{in} & \ldots & q_{en} & 0 \\
R_{ii} & 0 & \ldots & r_{ii} & \ldots & r_{en} & R_{en} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
R_{ni} & r_{ni} & \ldots & 0 & \ldots & r_{en} & R_{en} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
R_{ne} & r_{ne} & \ldots & r_{en} & 0 & R_{en} & 0 \\
0 & 0 & \ldots & 0 & \ldots & 0 & 1
\end{pmatrix}
\]

where \( q_x = q_{01} + \ldots + q_{in} + \ldots + q_{en} \).

2.2. Probabilities of AIS transition into various states

Let us determine probabilities of AIS transition into various states as per matrix (1).

After the first step, probabilities of states will be as follows:

\[
P_0(1) = 1 - \sum q; P_1(1) = q_{01}; \ldots; P_i(1) = q_{0i}; \ldots; P_n(1) = q_{0n}; P_{n+1}(1) = 0.
\]

Probabilities of states in the subsequent steps will be as follows:

\[
P_0(k) = \sum_{j=0}^{n+1} P_j (k-1)P_{j0} = P_0(k-1)P_{00} + P_1(k-1)P_{10} + \ldots + P_n(k-1)P_{n0} + P_{n+1}(k-1)P_{n+1,0};
\]

\[
P_1(k) = \sum_{j=0}^{n+1} P_j (k-1)P_{j1} = P_0(k-1)P_{01} + P_1(k-1)P_{11} + \ldots + P_n(k-1)P_{n1} + P_{n+1}(k-1)P_{n+1,1};
\]

\[
P_i(k) = \sum_{j=0}^{n+1} P_j (k-1)P_{ji} = P_0(k-1)P_{0i} + P_1(k-1)P_{1i} + \ldots + P_n(k-1)P_{ni} + P_{n+1}(k-1)P_{n+1,i};
\]

\[
P_n(k) = \sum_{j=0}^{n+1} P_j (k-1)P_{jn} = P_0(k-1)P_{0n} + P_1(k-1)P_{1n} + \ldots + P_n(k-1)P_{nn} + P_{n+1}(k-1)P_{n+1,n};
\]

\[
P_{n+1}(k) = \sum_{j=0}^{n+1} P_j (k-1)P_{j,n+1} = P_0(k-1)P_{0,n+1} + P_1(k-1)P_{1,n+1} + \ldots + P_n(k-1)P_{n,n+1} + P_{n+1}(k-1)P_{n+1,n+1};
\]

It follows from (3) that after \( k \)th step probability of successful outcome produced from dependent threats’ effecting AIS will be equal to:

\[
P_{so}(k) = P_0(k) + P_1(k) + \ldots + P_i(k) + P_n(k).
\]

Probability of the opposite event, i.e. of unsuccessful outcome will be equal to:

\[
Q_{BH}(k) = P_{n+1}(k).
\]

Since \( P_{so}(k) \) and \( Q_{so}(k) \) constitute a complete group of events, then:

\[
P_{so}(k) + Q_{so}(k) = 1.
\]

Formula (6) is used as a verification rule.

2.3. Mathematical modelling to assess security of restricted-access information

The following characteristics are used as input parameters:
• number of threats (N) in question characterizing the number of threats in the current list of threats;
• number of steps of algorithm (K) characterizes the time of threats’ effecting RAI. Since the method selected for measuring RAI security is discrete, then algorithm itself is considered stepwise (1, 2, … K);
• matrix of transition probabilities \( \| P_{ij} \| \), presented in figure (1), characterizes a source graph of AIS states, namely:
  1) \( q_{01}, \ldots, q_{0i}, \ldots, q_{0n} \) – probability of \( i^{th} \) threat occurrence;
  2) \( R_{10}, \ldots, R_{1i}, \ldots, R_{1n} \) - probability of correcting \( i^{th} \) threat occurred;
  3) \( \overline{R}_{1n+1}, \overline{R}_{2n+1}, \ldots, \overline{R}_{K,n+1} \) - probability of failure to correct \( i^{th} \) threat occurred;
  4) \( r_{i,j} \) – probability of generating \( j^{th} \) threat to RAI security when carrying out \( i^{th} \) threat.

As a result of measuring RAI security against law-breaker’s carrying out various threats using software, the following output parameters are formed:
• matrix \( \| B_{ij} \| \), probabilities of which characterize capacity of the system to be in any out of 0, 1, ..., \( n, n+1 \) states at each \( K \) step of algorithm (for instance, \( b_{ij} \) specifies that the system will be at the \( i^{th} \) step of algorithm at \( j^{th} \) state with probability \( b_{ij} \));
• probabilities of successful outcome \( (P_{so}) \) and unsuccessful outcome \( (Q_{so}) \) produced from carrying out threats, and, respectively, calculated for each \( K \) step of algorithm;
• graph representation of relationship between \( P_{so} \) and \( K \) steps of algorithm.

Flow-chart of algorithm is presented in figure 2.
As per figure 2, flow chart is made taking into account quantitative assessment of RAI security for dependent flows of threats, input parameters, and output parameters formed by the software.

As per figure 2, an algorithm and software were developed [13]. To implement algorithm for quantitative assessment of RAI security, Delphi programming system is selected because it has the widest potential for programming Windows OS applications.

3. Results

To study the effect produced by parameters that characterize security of RAI, and the number of algorithm steps, on the value of successful outcome probability, modelling was performed for three modes (tests) presented in figure 3 in the form of matrices of transition probabilities. Figures 3 show several different sets of input parameters with various parameters of probabilities of threats occurrence, correction probabilities, and probabilities of threats cross-generation.

The study results are shown in figure 4.
Analysis of figure 4 allows to arrive at the following main conclusions:

- A relationship between probability of successful outcome and probability of threats occurrence has on the value of successful outcome probability. Figure 5 show several different sets of input parameters with various parameters of probabilities of carrying out threats, correction probabilities, and probabilities of threats cross-generation.

The study results are presented in figure 6. Analysis of figure 6 allows to infer as follows:

1. A relationship between probability of successful outcome and probability of - q threat effecting AIS and the number of algorithm steps - K is obtained.
2. The first mode of tests is characterized by 0,04 probability of q threats occurrence, second: 0,08; third: 0,14; and fourth: 0,25. The more steps modelling involves, and the more are the values of probability of threats effecting AIS, the less are the values of probability $P_{so}$. Thus, for instance, at the
15th step of the algorithm probability $P_{so}$ for $q = 0.04$ is 0.78, for $q = 0.08 P_{so} = 0.63$, for $q = 0.14 P_{so} = 0.5$, and for $q = 0.25 P_{so} = 0.36$.

![Figure 6](image.png)

**Figure 6.** Relationships between successful outcome $P_{so}$ and probability of occurring threats -$q$ and number of steps of algorithm – $K$

3. The studies conducted indicate that an owner of RAI shall take into consideration both capacities of law-breakers to have unauthorized access to RAI (through probability $q$ of carrying out threats), and its capacities to protect information resources (through probability $R$ of correcting threats) while organizing and implementing in practice protection mechanisms held by an owner of RAI.

4. **Discussion**

The results obtained in the paper may be interpreted as follows. Analysis of literature references presented in the paper shows that the problem of quantitative assessment of RAI security is rather relevant. At the same time, the analysis also shows that the problem of RAI security, taking into account the effect produced by inside and outside threats on AIS, is currently of special importance and interest. This is because law-breaker’ carrying out both inside, and outside threats is dangerous in terms of material and moral damage inflicted on an owner of RAI.

A basis for the method suggested is that in the process of using AIS, it withstands an impact of inside and outside threats of various origins. Resulting from such impacts, the system may pass into various states with successful and unsuccessful outcomes. The method enables to compose a matrix of the system transition from one state to the other, determine probabilities of such transitions, and define thereupon probabilities of successful and unsuccessful outcomes in question. With these probabilities at hand, an owner of RAI has an opportunity for taking organizational and prevention measures to protect its information resources. Upon that, an owner of RAI shall take into account the following obtained results:

- compute probability of successful (unsuccessful) outcome using this method for each threat effecting AIS;
- arrange the values of obtained probabilities in ascending (descending) order;
- identify the most dangerous threats;
- make a decision on improving the existing system of securing RAI.

5. **Conclusion**

The paper illustrates the growing importance of RAI security problem since there is a serious gap between realizing a need for preventing danger of RAI leak and launching the means, methods, and measures used to protect RAI that, in its turn, is caused by difficulties associated with lack of effective enough technological solutions and required financial resources as well. Thus, generally, the analysis is indicative of a vast disparity between highly assessed danger of inside and outside threats and measures taken to prevent them. Studies show that assessing RAI security using quantitative approach based on probabilistic criteria offers the greatest perspectives.
If a problem implies that Markov random process with discrete states is used, transition of AIS from one state to the other occurs abruptly, almost instantaneously. For the conditions stated, the time for correcting threats is considerably lesser than AIS time for the i\textsuperscript{th} threat. The point here is that a particular outcome of the i\textsuperscript{th} threat effecting AIS is produced simultaneously with the moment of facing this threat.

Mathematical methods for studying RAI security taking into account impacts of threats on AIS based on Markov random processes with discrete states have been developed. It is shown that Markov random process with discrete states is characterized with a quality with no consequences that implies that transitions of AIS from one state to the other are possible at the fixed moments of time. In between these moments, the system retains its state. A mathematical model for assessing effect of threats on RAI security has been developed suggesting that if there are known probabilities of transitions into any other state for each AIS state, it is possible to compile a matrix of transition probabilities. With this matrix at hand, formulas to determine probability of AIS states after k\textsuperscript{th} step of transition from i\textsuperscript{th} into j\textsuperscript{th} state may be obtained.

**References**

[1] Buldyrev S V, Parshani R, Paul G, Stanley H E and Havlin S 2010 Catastrophic cascade of failures in interdependent networks *Nature* **464**(7291) pp 1025-8

[2] Tikhomirov A, Afanasyev A, Kinash N, Trufanov A, Berestneva O, Gnatyuk S and Umerov R 2014 Network Society: Aggregate Topological Models *Communications in Computer and Information Science* **487** pp 415-21

[3] Musa J D 2011 Software reliability Wiley Interdisciplinary Reviews: Computational Statistics **3** 269-81

[4] Galindo F, Dmitrienko N V, Caruzo A, Rossodivita A, Tikhomirov A A, Trufanov A I and Shubnikov E V 2010 Modelling of advanced attacks on integrated networks *Security of information technologies* **3** pp 115-21

[5] Lai Y C 2012 Security of complex networks FA9550-07-1-0045. 18-02-2010 Arizona State University, Tempe, AZ. AFRLOS-VA-TR-2012-0082. 15 p

[6] Threats to internal IT threats in Russia. Research company Info Watch www. Info Watch.ru/ (date of reference 11.11.2017/ дата обращения 11.11.2019).

[7] Tikhomirov A A and Trufanov A I 2011 Supercomplex networks: new models of interpreting social-economic and biosociological processes *Proceedings of RAN Institute of State and Law*. 6 pp 162-70

[8] Silowash G 2012 *Common Sense Guide to Mitigating Insider Treats 4th Edition* (Pittsburg: CERT Program) 144 p

[9] Cummings A 2012 *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* (Pittsburg: CERT Program) 76 p

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

[11] IBM SPSS Modeler 16 Algorithms Guide – 2013 [Web resource] URL: ftp://public.dhe.ibm.com/software/analytics/spss/documentation/modeler/16.0/en/AlgorithmsGuide.pdf (date of reference 11.11.2017/ дата обращения 11.11.2019).

[12] Bulyinski A V and Shiryaev A N 2005 The theory of random processes *Fizmatlit*

[13] Zhyryanov Y U Information Security of ERP-system. URL: http://citforum.ru/gazeta/49/ (date of reference 11.11.2017)/ Informatsionnaya bezopasnost' ERP-sistem. URL: http://citforum.ru/gazeta/49/ (date of reference 11.11.2017/ дата обращения 11.11.2019).

[14] Bjorn A G 2002 CORAS, A Platform for Risk Analysis on Security Critical Systems - Model-based Risk Analysis Targeting Security

[15] Boyd C and Mathuria A 2003 Protocols for Authentication and Key Establishment *Springer* **323**