Methods for Calculating Frequency of Maintenance of Complex Information Security System Based on Dynamics of Its Reliability

S K Varlataya¹, V E Evdokimov², A Y Urzov¹
¹School of Natural Sciences, Far Eastern Federal University, 10 Ajax Bay, Russky Island, Vladivostok 690090, Russia
²Peter the Great St.Petersburg Polytechnic University, 29 Polytechnicheskaya st., St. Petersburg 195251, Russia

E-mail: verronyvl@gmail.com

Abstract. This article describes a process of calculating a certain complex information security system (CISS) reliability using the example of the technospheric security management model as well as ability to determine the frequency of its maintenance using the system reliability parameter which allows one to assess man-made risks and to forecast natural and man-made emergencies. The relevance of this article is explained by the fact the CISS reliability is closely related to information security (IS) risks. Since reliability (or resiliency) is a probabilistic characteristic of the system showing the possibility of its failure (and as a consequence - threats to the protected information assets emergence), it is seen as a component of the overall IS risk in the system. As it is known, there is a certain acceptable level of IS risk assigned by experts for a particular information system; in case of reliability being a risk-forming factor maintaining an acceptable risk level should be carried out by the routine analysis of the condition of CISS and its elements and their timely service. The article presents a reliability parameter calculation for the CISS with a mixed type of element connection, a formula of the dynamics of such system reliability is written. The chart of CISS reliability change is a S-shaped curve which can be divided into 3 periods: almost invariable high level of reliability, uniform reliability reduction, almost invariable low level of reliability. Setting the minimum acceptable level of reliability, the graph (or formula) can be used to determine the period of time during which the system would meet requirements. Ideally, this period should not be longer than the first period of the graph. Thus, the proposed method of calculating the CISS maintenance frequency helps to solve a voluminous and critical task of the information assets risk management.

1. Introduction
Information security tasks do not cease to be relevant: on the contrary, increasing of information resources significance for economical development of enterprises, countries and the whole world makes a problem of constructing a reliable protection loop for information assets one of the primary. Approaches to information security change with time and today complex information security systems (CISS) are created to manage these problems. By their definition, these systems are complex, and, accordingly, the positions of the theory of complex systems can be applied to them. One of the key indicators of system quality is its reliability level. More details about reliability in information security...
sphere are available in sources [1-5], details about system reliability in general, models and assessment methods— in papers [6-10].

According to system reliability theory the reliability level represents probabilistic property of an object to keep in time within the established limits the values of all parameters characterizing the ability to perform the required functions in the given modes and conditions of application, maintenance, repair, storage and transportation [11]. Applied to CISS, reliability is a property of CISS which allows to provide information protection for a predetermined period of time. At the end of this period a system denial can occur, i.e. an event, which leads to inability of the system to perform its function. System reliability can also be called fault tolerance.

In this paper, we will consider the reliability characteristics of the CISS, its relationship with the risk of information assets, as well as the calculation of the reliability and maintenance period of the CISS.

2. Reliability of CISS

As mentioned before, system reliability is a probabilistic indicator, so in order to calculate its value we have to know reliability values of each separate system elements: CISS is decomposed on separate logically or technically integral blocks and then reliability of these elements is calculated. Depending on the type of connection of these blocks (parallel or serial) to calculate reliability common formulas can be used [12]:

\[ P_{\text{CISS}} = \prod_{i=1}^{K} P_i \text{ - for serial connection} \]  
\[ Q_{\text{CISS}} = \prod_{i=1}^{K} Q_i \text{ - for parallel connection} \]

where \( P_{\text{CISS}} \) – system reliability, \( Q_{\text{CISS}} \) – probability of system denial.

Because:

\[ P_{\text{CISS}} = 1 - Q_{\text{CISS}} \]  

system reliability when its blocks are connected parallel is determined by formula:

\[ P_{\text{CISS}} = 1 - \prod_{i=1}^{K} (1 - P_i) \]  

It is seen that systems with parallel connection of elements are much more reliable than systems with serial connection where failure of any element leads to denial of the whole system.

An important indicator of system reliability is a parameter called failure rate – number of failures per time unit in relation to the total number of system elements:

\[ \lambda(t) = \frac{n(\Delta t_i)}{N_{\text{mid}} \cdot \Delta t_i} \]

where \( n(\Delta t_i) \) – number of failures of same type objects on interval \( \Delta t_i \), on which is determined \( \lambda(t) \); \( N_{\text{mid}} \) – number of operable objects in the middle of the interval \( \Delta t_i \).

From this statement we can get following:

\[ P(t) = \exp[-\int_{0}^{t} \lambda(t) dt] \]
which represents a probability of trouble-proof operating of system element according to its reliability exponential model [13]: system element reliability chart is an exponentially decreasing curve (figure 1).

\[ P(t) = \exp(-\lambda t) \]  \hspace{1cm} (7)

**Figure 1.** System element reliability changing curve.

Based on the analysis, we can conclude that the highest level of system reliability can be achieved by parallel connection of main logically or technically integral blocks. In this case whole system failure probability is a multiplication of the system’s separate blocks failure probabilities and this value is less than a probability of the most unreliable system element failure. Since it is about parallel connection of just main system blocks which consist of a certain number of elements having their own reliability indicator, we cannot guarantee that all those elements is possible to integrate into a one-piece subsystem using parallel connection. Therefore when calculating system reliability we have to use mixed model for greater accuracy. It will be unique for each system. In common case we may describe a certain CISS which elements are connected as shown on figure 2.

**Figure 2.** Mixed type of CISS elements connection.

An example of such system is an unauthorized access prevention system representing \( n \) amount of information security means (ISM\(_1\)-ISM\(_n\)) installed on user’s workstations and having centralized management. Any ISM failure does not lead to failure of the whole system (due to parallel
connection). At that for instance physical damage of electronic circuit of IMS hardware module element \((E_{l_1} - E_{l_m})\) can cause IMS failure (due to serial connection).

The formula for such systems reliability calculation looks like this:

\[
P_{CISS} = 1 - \prod_{i}^{n} \left(1 - P_{SIM} \right) = 1 - \prod_{i}^{n} \left(1 - \prod_{k=1}^{m} P_{El_k} \right)
\]  \hspace{1cm} (8)

Then insert value \(P = \exp(-\lambda t)\) to the formula (8):

\[
P_{CISS} = 1 - \prod_{i}^{n} \left(1 - \exp[-\lambda_i t] \right)
\]  \hspace{1cm} (9)

or

\[
P_{CISS} = 1 - \prod_{i}^{n} \left(1 - \exp[-t \cdot \sum_{k=1}^{m} \lambda_k] \right)
\]  \hspace{1cm} (10)

Figure 3 represents CISS reliability changing chart:

![CISS reliability changing chart](image)

**Figure 3.** CISS reliability changing chart.

CISS reliability changing chart is a S-shaped curve where 3 time intervals can be divided: almost constant high level of reliability, a uniform reduction of reliability, almost constant low level of reliability. Setting the minimum acceptable level of reliability, the graph (or formula) can be used to determine the period of time during which the system would meet requirements. Ideally, this period should not be longer than the first period of the graph.

This chart demonstrates time dependence of common CISS reliability. As is seen there is a certain time frame \(\Delta t_1\) when reliability function \(P\) decreases slowly. Then an intensity of reliability drop increases abruptly on time frame \(\Delta t_2\), and after that (time frame \(\Delta t_3\)) \(P \sim \text{const}=\min\). At that \(\lambda\)-factor value (denial intensity) directly affects length of time frame \(\Delta t_1\) when \(P \sim \text{const}=\max\).

To determine value of a CISS reliability index, it is necessary to provide three most important properties of protected information: confidentiality, integrity and accessibility (CIA triad) [9]. In case of security system denial one or several of those properties may be violated. Considering that total risk for information assets is made up of individual risks:

\[
R_{\text{total}} = \sum_{i}^{m} R_i
\]  \hspace{1cm} (11)
we can talk of CISS denial as a threat realization, which existence produces one of \( m \) risks for information assets. During risk analysis CISS reliability factor should be taken into account and minimum sufficient level of reliability should be set to make total risk be within norm. Knowing the values of failure intensity \( \lambda_i \) for system elements (these parameters are set by a producer) we can determine a time period \( T_{eff} \) while the system operates the most stable. This time period should be considered when setting a period of CISS maintenance to keep its stable and effective operating.

3. Conclusion

Thus, this article describes the calculation of complex information security system reliability, demonstrates system reliability change in time, and determines an ability of calculating the maintenance period of CISS based on its reliability index.

References

[1] Jóźwiak I and Laskowski W 2008 A short note on reliability of security systems Reliability & Risk Analysis: Theory & Applications 2(1) pp 88–94
[2] Scheglov A and Scheglov K 2005 Introduction to the theory of information security reliability The tasks of reserving security mechanisms Sec.ru publications
[3] Gromov Y Y 2010 Reliability of information systems (Tambov: TSTU publishing)
[4] Malkov M V 2012 About reliability of information systems Kola Science Centre of RAS publications P3 4 pp 49–58
[5] Bulgakov O M, Udalov V P and Kuchmasov E A 2012 Principles of constructing the reliability model of the information security system Bulletin of the Voronezh Institute of the MOI of Russia 3 pp 167–176
[6] Boyko O G and Shaimardanov L G 2009 Mathematical models and methods for calculating the reliability of complex systems Issues of modern science and practice 8(22) pp 64–72
[7] Pereguda A I and Timashov D A 2010 Evaluation of reliability indices of an automated technological complex “protection object - security system” with fuzzy parameters by the Monte Carlo method Scientific session of MEPI-2010. Information and telecommunication systems. Problems of information security pp 144–147
[8] Pereguda A I and Tverdokhllebov R E 2004 Mathematical model of reliability of information systems Methods of quality management 6 pp 39–44
[9] Barlow R E and Proschan F 1996 Mathematical theory of reliability (Philadelphia: SIAM)
[10] Kalimulina E Y 2008 Calculation of the reliability of complex systems with a parallel structure, fully recoverable during operation “Managing large systems” ICS RAS Collection of Articles 23 pp 156–170
[11] GOST 27.002-89 Industrial product dependability. General principles. Terms and definitions
[12] Dmitriev Y V 2013 Reliability of structures and bases of transport structures (Khabarovsky: FESTU Publishing)
[13] Shapoval V V 2000 Basics of working capacity of technical systems (Vladivostok: VVSU publishing) p 3