Mathematical Model for Collecting and Evaluating Complex Security Factors and Ensuring the Prevention of Threats to Individuals and Society in Cyberspace

Denis V. Poltoranov[1,*] and *Tatiana V.* Karlova[2,**]

[1]Institute For Design-Technological Informatics RAS, RU-127055, Moscow, Russia
[2]Moscow State Technological University "STANKIN", RU-127055, Moscow, Russia

Abstract. This article is devoted to the development of a model and elaboration of the structure of the mathematical formalism for the assessment of the state of comprehensive security in order to prevent threats to the individual and society in cyberspace. The types and objects of information threats are examined, the main properties, which are indicators and parameters we should possess, are revealed and the key stages of status assessment of comprehensive security in state entities, municipalities and organizations are identified.
Keywords. information security, comprehensive security, status assessment, indicators, information threats.

1. Introduction

The system of comprehensive security of each state is a set of bodies and institutions that function in the areas of regulation, prevention and elimination of the consequences of various threats (political, economic, biological, chemical, environmental, etc.). In Russia there is a system of ensuring national security, consisting of state and non-state subsystems. The state system is formed by legislative, executive, and judicial state institutions that take part in the process of making decisions and implementing political, legal, organizational, economic, military, and other measures aimed at ensuring the security of the individual, society, and the state. The non-state system consists of public associations, which include the media and individuals who can influence the formation and implementation of national security policies. The concept of security is a multi-vector and multidimensional concept, which includes a whole set of structural components. [1,2]

The integrated security system of each State consists of the bodies and institutions that operate to regulate, prevent and respond to various threats (political, economic, biological, chemical, ecological and others). The Russian Federation has a national security system consisting of State and non-State subsystems. The State system shall form legislative, executive and judicial State institutions that take part in the process of formulating decisions and implementing measures of a political, legal, organizational, economic, military or other nature; aimed at ensuring the security of individuals, society and the State. The non-State system consists of voluntary associations, which include the media and private individuals who can influence the formulation and implementation of national security policies. The concept of security is a multidimensional and multifaceted one that incorporates a variety of structural components.

Assessing the state of comprehensive security to prevent threats to the person and society in cyberspace is one of the most important tasks that the state solves. Currently, there are no approved methods or recommendations for assessing the state of comprehensive security to prevent threats to the person and society in cyberspace, and the existing international recommendations do not take into account the specifics of the Russian Federation. The types and objects of threats in cyberspace are shown in table 1. [3,4]

Table 1. Objects and types of cyber threats

Source of Threat	Types of Threat
External	
Activities of foreign intelligence and intelligence services, criminal groups and formations	Obtaining unauthorized access to information and monitoring the functioning of information systems; interception and leakage of information through technical channels; (not)controlled distribution of computer viruses and other malicious programs
Illegal activities of individuals	
Internal	
Violation of established regulations on the collection, processing and transmission of information	Leakage/disclosure of information constituting a state, official, or other type of secret; possession of personal data (including financial data) of the company/person; failure, failures, malfunctions of
Intentional actions and unintentional errors of information systems personnel	

e-mail: *depo768@rambler.ru, **karlova-t@yandex.ru

Use of unlicensed software, involvement of persons who do not have a license for this type of activity in the creation of information systems of the organization	technical means, information security programs; failures of technical means and software failures in information and telecommunications systems
Transboundary	
Development of cybercrime (financial, piracy, distribution of pornographic and extremist content)	Cardering, Internet acquiring crimes, fraud, illegal business on the Internet, acquisition of intellectual property, recruiting members of international terrorist and extremist groups
Functioning of unlicensed financial institutions and online trading platforms	Conclusion of counterfeit agreements, money laundering, illegal seizure of other people's property

2. Theoretical basis

The theoretical basis of this work was the national scientific works of Russian and foreign scientists on development information management and its subjects, as well as methods, principles and models of historical, genetic and systemic approach the legal and regulatory framework of the Russian Federation and individual States on issues of ensuring state and public security, including in cyberspace; scientific works of T.V. Vladimirova, R.I. Vylkov, A.A. Kalinkin, A.I. Kovaleva, M.A. Petlin, I.Yu.Sayapina and many other domestic and foreign researchers.

3. Discussion

In the methodology presented below, the assessment of the state of comprehensive security to prevent threats to the individual and society in cyberspace (hereinafter referred to as the comprehensive security) is expressed by an integral dimensionless indicator, determined in the range from 0 to 1 and showing the probability with which the integrated security of the object of assessment is ready to perform tasks on destination. In this article, the object of assessment means a federal executive body, a constituent entity of the Russian Federation, a municipality or an organization.

The considered integral indicator of the state of complex security is the upper level of the hierarchy shown in Figure 1, and is determined based on the values of indicators of the state of complex security.

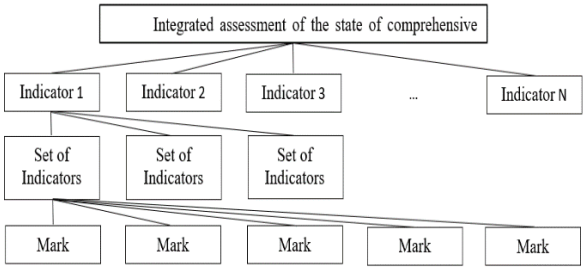

Fig. 1. Hierarchy used to assess the state of comprehensive security.

These indicators should have the following properties:

- reliability - the indicator should characterize progress in achieving a goal or solving a problem and cover the maximum number of aspects of achieving the goal or solving complex security problems;
- objectivity - it is necessary to use indicators that reflect the real state of affairs;
- unambiguity - the definition of the indicator should provide the same understanding of the essence of the measured characteristic, exclude the possibility of double interpretation or understanding;
- cost-effectiveness - reporting data should be obtained at the lowest possible cost, and the indicators used should be based as much as possible on existing procedures for collecting information in the field of comprehensive security;
- reliability - the method of collecting and processing the initial information should allow the possibility of verifying the accuracy of the data obtained;
- timeliness and regularity - to be used for monitoring purposes, reporting data should be updated at least once a year. [5]

Taking into account the above properties, the following indicators of the state of integrated safety are established (depending on the object of assessment, indicators can be supplemented or reduced):

- protection of the individual (society, state);
- readiness of the management system of security agencies;
- the readiness of the security forces;
- stability of functioning of economic objects.

The values of the groups of indicators are calculated by aggregating the corresponding marks of the state of integrated security, which are collected within the framework of information exchange.

Mathematically, such a hierarchy (Figure 1) can be written as:

$$I = f(I_1 \dots I_n); \quad I_n = f(M_1^n \dots M_k^n); M_k^n = f(m_1 \dots m_i), \tag{1}$$

where: n – is the number of indicators;

k – number of indicator groups corresponding to the I_n indicator;

i – is the number of marks corresponding to the M_k^n indicator group.

Among the basic principles underlying the theory of management, the central place belongs to the hierarchical subordination in the activities of various systems at various levels. [6,7]

If, as an integral indicator of assessing the state of comprehensive security, the probability of developing instability in society is taken, then various scales can be used to assess the state of comprehensive security: "unstable" - from 0 to 0.7; "Satisfactory" - from 0.7 to 0.8; "Stable" - from 0.8 to 1.

In the following methodological approach to assessing the state of comprehensive security, the Harrington desirability scale is used: "Very bad" 0.00 - 0.20; "Bad" 0.20 - 0.37; "Satisfactory" 0.37 - 0.63; "Good" 0.63 - 0.80; "Very good" 0.80 - 1.00. The choice of marks 0.37 and 0.63 on the desirability scale is explained by the convenience of calculations, since the desirability function is exponential:

$$0{,}37 = \frac{1}{e} \; ; \; 0{,}63 = 1 - \frac{1}{e} \quad . \tag{2}$$

Comprehensive security assessment is carried out in four stages:

Stage 1: "Determination of marks of the state of comprehensive security".

Stage 2: "Calculation of the groups of indicators".

Stage 3: "The calculation of indicators."

Stage 4: "Calculation of the integrated assessment of the state of comprehensive security".

At the 1st stage, the marks of the state of comprehensive security of the object of assessment are collected. This stage can be considered as a preparatory stage, the reliability of the assessment directly depends on the reliability of the information collected at this stage.

Then, at stage 2, the values of groups of indicators are calculated. Due to the fact that only those that meet the requirements presented above are selected as marks of the state of comprehensive security required for its assessment, the values of the groups of indicators express the share of security (need – actual availability) or the share in the total amount. Accordingly, the values of the indicator groups are in the range from 0 to 1.

At the 3rd stage, the values of the indicators of comprehensive security status are calculated. One of the methods of the theory of experiment planning has been adapted as a methodological basis for this calculation. The value of the generalized Harrington desirability function is taken as the indicator value. This approach, based on the assessment of processes on the Harrington scale of importance, is widely used in quality management systems of organizations to assess their effectiveness. [8]

The calculation sequence of the indicator is as follows:

3.1. Coding the values of indicator groups.

3.2. Calculation of particular values of the desirability of groups of indicators.

3.3. Calculation of the indicator value.

On sub-stage 3.1, the resulting values of indicator groups are coded or, in other words, scaled. This allows to set lower and upper permissible limits of integrated security readiness measurements for different objects of assessment.

Let's give an example: the readiness of comprehensive security in a border state entity of 0,6 can be estimated as "not ready", while the same readiness value for another entity can correspond to the assessment "limited ready".

Thus, the translation of the values of the groups of indicators M into the conditional scale M ' is carried out in order to evaluate various objects of assessment on the same scale. Dependencies for coding:
for state entities, municipalities that are not assigned to civil defense groups, and organizations that are not assigned to civil defense categories by (3):

$$M' = 9{,}73 \cdot M - 5{,}13 \quad , \tag{3}$$

for state entities, municipalities assigned to civil defense groups, and organizations assigned to civil defense categories by (4):

$$M' = 12{,}25 \cdot M - 7{,}65 \quad . \tag{4}$$

An explanation of the form of equations (3) and (4) and the values of the corresponding coefficients is given below.

On sub-stage 3.2 by (5), particular values of desirability of groups of indicators d_M are calculated by (5):

$$d_M = \exp(-exp(-M')) \; , \tag{5}$$

It is assumed that the relationship between the indicator value and its encoded value is linear, so:

$$M' = a_1 \, M + a_0 \; . \tag{6}$$

The coded value of M' is expressed from (5) by double logarithm:

$$\ln \ln \left(\frac{1}{d}\right) = - M' \; . \tag{7}$$

Substituting the value of M' in (6), we obtain:

$$a_1 \, M + a_0 = \ln \left(\frac{1}{\ln \left(\frac{1}{d}\right)} \right) \; . \tag{8}$$

For the minimum and maximum desirable value of the group of indicators M_{min} and M_{max}, respectively, it is possible to create a system of equations (8)

$$\begin{cases} a_1 \, M_{min} + a_0 = \ln \left(\frac{1}{\ln \left(\frac{1}{d_{min}}\right)} \right) \\ a_1 \, M_{max} + a_0 = \ln \left(\frac{1}{\ln \left(\frac{1}{d_{max}}\right)} \right) \end{cases} . \tag{9}$$

The coefficients a_1 and a_0 used in (3) and (4) are expressed for (9).

On sub-stage 3.3 (10), the value of the indicator I_n is calculated as the geometric mean of the particular values of the desirability of the groups of indicators d_M, taking into account their significance.

$$I_n = \sqrt[k]{\prod^{k} d_M^{\beta}} \qquad (10)$$

where: k – is the number of indicator groups that make up the I_n indicator;

β – coefficient of significance of a group of indicators.

The value of the coefficient of significance of a group of indicators is determined by (11) based on its rank assigned according to the results of a survey of experts (1 is the most significant, then in decreasing order of importance) [9]:

$$\beta = \frac{u}{2^{u-1}}, \qquad (11)$$

where: u – the rank of the group of indicators.

The β values for ranks 1 to 9 are shown in Table 2.

Table 2. Significance coefficient Values for ranks 1-9

Significance coefficient β	Rank u
1	1
1	2
0.75	3
0.5	4
0.3125	5
0.1875	6
0.11	7
0.063	8
0.035	9

After determining the values of all groups of indicators, an integral assessment of the state of comprehensive safety is determined at stage 4.

The calculation sequence for its definition is the same as stage 3 and can be presented in three sub-stages:

4.1. Coding of indicator values as per (3) or (4).

4.2. Calculation of the particular values of the desirability of the indicators according to (5).

4.3. Calculation of the value of the integral estimate according to (10).

4. Results and Discussion

In today's world of multiple threats, the concept of security is multidimensional and encompasses many facets of everyday life. Today, many individual spheres of life must be properly regulated and monitored by the State in order to sustain human life. Depending on the type of existing threats, there are also different subspecies of security: national, economic, energy, environmental, etc. According to the number of subjects, the security of the individual, society, and the state is distinguished. In fact, the state's activities are aimed at ensuring the security of the individual and society. Ensuring such security is regulated through the prism of legal regulation and the functioning of the entire system of state and municipal authorities. Depending on existing threats, each State develops its own strategies for the protection of its citizens and its territorial integrity. In the Russian Federation, this strategy has been adopted at the federal level and supplemented by acts of the constituent entities. The concept of comprehensive state security is aimed at creating a system of tools (authorities, services, etc.) which, taken together, are capable of preventing and resolving all kinds of threats to the rights and freedoms of the individual, society and the State. [9, 10]

In conclusion, it should be noted that the advantage of using the described methodological approach is the possibility of using different ranges when assessing the state of integrated safety of various objects of assessment without making changes to the mathematical formalism. In addition, the desirability function has such useful properties as continuity, monotony and smoothness, is not sensitive at extreme values, and reflects well the estimate in the middle zone.

The proposed mathematical model for collecting and evaluating complex security factors and ensuring the prevention of threats to individuals and society in cyberspace may be of interest to specialists in the field of information threats to qualitatively assess the problems of the state of an object.

References

1. Z. Bangwei, Interdisciplinary Description of Complex Systems, **17**(3), 520-545 (2019) https://doi.org/10.7906/indecs.17.3.13
2. G.A. Makeev, Computer Science and Information Technologies (CSIT'2014) Proceedings of the 16th International Workshop, 101-104 (2014)
3. D.V. Poltoranov, QUALITY. INNOVATION. EDUCATION., **4**(162), 60-66 (2019) [in Russia]
4. T. Karlova, A. Bekmeshov, N. Kuznetsova, 2019 International Conference «Quality Management, Transport and Information Security, Information Technologies» (IT&QM&IS) (2019) doi:10.1109/itqmis.2019.8928412
5. P.A. Knyazev, D.V. Poltoranov, Civil Security Technologies, **13**(2), 92-97 (2016) [in Russia]
6. V.K. Fedyukin *Quality Management of Technological Processes.* (M.: KNORUS, 2013)
7. V. Karlova, E. A. Kirillova, A .Y. Bekmeshov, A.N. Zapolskaya, I .A. Mikhaylov, 2019 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) (2019) doi:10.1109/itqmis.2019.8928381
8. R.V. Butkevich, Yu.S. Klochkov, T.S. Yanitskaya, S.A. Yarygin Bulletin of the Samara Scientific Center of the Russian Academy of Sciences, **7**(2), 456-463 (2005) [in Russia]

9. T. K arlova, M . Mikhaylova, N . K uznetsova, A. Bekmeshov, D. Poltoranov, E. Obukhova, EPJ Web of Conferences **224**, 0600 4 (2019) https://doi.org/10.1051/epjconf/201922406004
10. A.F. Nevostrueva, Global Media Journal, **1** (2016)