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

Denis V. Poltoranov1,* and Tatiana V. Karlova2,**

1Institute For Design-Technological Informatics RAS, RU-127055, Moscow, Russia
2Moscow 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 media and individuals who can influence the formation and implementation of national security policies. The concept of information security is a multi-dimensional 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 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 cyber threats are shown in Table 1.

| 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 |                  |

Table 1. Objects and types of cyber threats

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
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 to 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 Russian and foreign scientists on the theoretical basis of this work; as well as participation 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.

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.

2.1. Transboundary

Functioning of unlicensed financial institutions and online trading platforms.

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.

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 integrated in dimensionless indicator, determined at the lowest possible cost, and the indicators should provide the same understanding of the essence of the measured characteristic, exclude the possibility of double interpretation or understanding; the measured characteristic should reflect the real state of affairs; these indicators should have the following properties:

- objectivity - it is necessary to use indicators that reflect the real state of affairs;
- unambiguity - the definition of the indicator in the context of the methodology presented below, the assessment of the state of integrated safety is 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:

\[ I = f (I_1 \ldots I_n); \]

\[ I_n = f (M_1^n \ldots M_k^n); M_k^n = f (m_1 \ldots m_l), \]

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 assessment of comprehensive security, the central place belongs to the hierarchical subordination in the activities of various systems at various levels. [6,7]

Identification of an integral indicator of 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:

\[
0.37 = \frac{1}{e} ; \quad 0.63 = 1 - \frac{1}{e} . \tag{2}
\]

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

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

At the first 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 are required for the assessment, the values of the groups of indicators express the share of security (need - actual availability) or the state 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 assigned to civil defense groups, a nd organizations t hat are not assigned to civil defense categories by (3):

\[
M' = 9.73 \cdot M - 5.13 \tag{3}
\]

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

\[
M' = 12.25 \cdot M - 7.65 \tag{4}
\]

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

The coded value of the 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:

\[
a_1 \cdot M + a_0 = \ln \left(\frac{1}{\ln \left(\frac{1}{d}\right)}\right). \tag{8}
\]

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):

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

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.

$$I_n = \sqrt[k]{\prod_{M=1}^{k} d_M^\beta} \quad (10)$$

where: $k$ is the number of indicator groups that make up the $I_n$ indicator; 
$\beta$ is the 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 decreasing order of importance) [9]:

$$\beta = \frac{u}{\sum u} \quad , \quad (11)$$

where: $u$ is the rank of the group of indicators.

The $\beta$ values for ranks 1 to 9 are shown in Table 2.

**Table 2.** Significance coefficient Values for ranks 1-9

| Rank $u$ | Significance coefficient $\beta$ |
|---------|-------------------------------|
| 1       | 1                             |
| 2       | 0.75                          |
| 3       | 0.5                           |
| 4       | 0.3125                        |
| 5       | 0.1875                        |
| 6       | 0.11                          |
| 7       | 0.063                         |
| 8       | 0.035                         |
| 9       | 0.015                         |

After determining the values of a ll g roups o f indicators, a n 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:

1. **Coding of indicator values** as per (3) or (4).
2. **Calculation of the integral estimate** of the desirability of the indicators according to (5).
3. **Calculation of the value of the integral estimate** according to (10).

### 4. Results and Discussion

In today’s world, multiple threats, economic, security and other facets of everyday life. Today, many in 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 act ivities a re ai med at ensuring t he security o f t he individual a nd s ociety. Ensuring such security is regulated through the prism of legal regulation and the functioning of the state system of local 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 described methodological approach is that it makes possible to use 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 useful properties such as continuity, monotony and smoothness, which is reflected well in the estimate in the middle zone.

The proposed mathematical model for collecting and evaluating complex security factors associated with cyber 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. B angwei, Interdisciplinary Description of Complex Systems, **17**(3), 520-545 (2019) [https://doi.org/10.7906/indecs.17.3.13](https://doi.org/10.7906/indecs.17.3.13)
2. G.A. M开采, Computer Science and Information Technologies «CSIT’2014» Proceedings of the 16th International Workshop, 101-104 (2014)
3. D.V. P oltonarov, QUALITY. INNOVATION. EDUCATION., 1**(1)**, 60-66 (2019) [in Russian]
4. T. Karlova, A. B ekmeshev, N. Kuznetsova, 2019 International Conference «Quality Management, Transport and Information Security. Information Technologies» (IT&QM&IS) (2019) [doi:10.1109/itqmis.2019.8928412](https://doi.org/10.1109/itqmis.2019.8928412)
5. P.A. K nyazev, D.V. Poltoranov, C ivil Security Technologies, 1**(3)**, 92-97 (2016) [in Russian]
6. V.K. F edyukin Quality Management of Technological Processes. (M.: KNORUS, 2013)
7. V. K. arlova, E. A. K irillova, A. Y. Bekmeshev, A.N. Zapolskaya, V. A. Mikhaylov, 2019 1 International Conference “Quality Management, Transport and Information Security. Information Technologies” (IT&QM&IS) (2019) [doi:10.1109/itqmis.2019.8928381](https://doi.org/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 Russian]
9. T. K. Karlova, M. Mikhailova, N. Kuznetsova, 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)