UDC 004.021 **DOI:** 10.18372/2310-5461.39.13087

V. V. Kozlovskii, Doctor of engineering, Professor
National aviation university
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com

O. V. Ivanov, Head of Foreign Affairs Department
National aviation university,
orcid.org/0000-0001-6550-4419
e-mail: alexkorea5@gmail.com

V. V. Snizhko, postgraduate student
National aviation university
orcid.org/0000-0002-8767-9073
e-mail: bb_c@ukr.net

ANALYSIS AND SECURITY MANAGEMENT OF TELECOMMUNICATION SYSTEMS BASED ON PREDICTIVE TECHNOLOGIES

Introduction

Solving of problems of information security and information security management is becoming vital to the existence and development of any modern organization.

Security is a comprehensive concept and can not be viewed as the sum of its parts. These parts are interconnected and interdependent [1]. In addition, each of these parts is critically significant. Consequently, the methods that involve partial neglect of safety criteria in overall safety assessment are unacceptable. Therefore, the development of the algorithm that allows unifying the approaches of integrated security system management is an urgent task.

Analysis of published data and problem definition

Security is a state and trends of development of protection of critical systems from external and internal negative factors. It is necessary to consider that security is a dynamic multiple objective category [2]. Security activities arise in the course of solving the contradiction between the risk and the need to manage the security: predict, prevent, eliminate and localize the damage from the impact of threats [3]. Comprehensive Security Assessment (CSA) cannot be more than conservative estimates obtained for different aspects of the system [4].

Security does not exist by itself, without human influence. It is provided for people and it is estimated by them. Therefore, the concept of security is not only objective, but also subjective, because of its evaluation carried out in the end by human [5]. The specific features of the task of creating security systems are [6]:

- incomplete initial information about the composition and nature of threats;
- complex problem of the need to take in account a large number of local indicators;
- presence of both quantitative and qualitative indicators that must be considered in solving problems of design and implementation of security systems;
- inability to use the classical optimization methods [7].

Cognitive analysis of the research object allows [8]:

- to predict the direction of the system (situation) development;
- to identify the factors, which affecting the situation;
- to formalize the decision-making processes;
- to get both qualitative and quantitative characteristics of the situation;

Information risk assessment, which is based on fuzzy cognitive modeling allows [9]:

- to identify the most dangerous threats and vulnerabilities affecting the telecommunication system;
- to assess possible damage from the effects of threats to telecommunication system;
- to adapt to new external and internal threats and technologies;

- to provide a simple and effective mechanism for decision-making services, dealing with information security.

Development of an algorithm that will unify approaches of integrated security managing will solve a number of issues related to the subjective side in the analysis and management of integrated security [10]

The aims and objectives of the research

The aim is to develop an algorithm of analysis and integrated security management based on cognitive modeling. This algorithm will unify approaches in constructing telecommunication security systems.

To achieve this goal it is necessary:

1. To form a matrix, by which the integrated security level can be described.
2. To form a matrix of preventive measures.
3. To form the matrix through which the implementation of preventive measures will be formalized.
4. Present the evaluation of integrated security system in the form of fuzzy cognitive model.

Development of algorithm of analysis and integrated security management

Let's formulate a mathematical model describing the dynamics of changes in the level of integrated security of different systems.

The integrated security level of a system is estimation, based on a set of indicators and criteria that characterize the state of the system in terms of protection of its critical elements.

The integrated security level of a system can be described by such a matrix (security matrix):

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ -- & -- & -- & -- & -- \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix}$$

where K_i — the security level of i^{th} criterion; F_i — trend of changes of i^{th} criterion (increases, decreases, neutral); V_i — the speed of changes of i^{th} criterion (low, below average, average, above average, high); T_i — the time, which is characteristic for i^{th} criterion, which can correctly interpret the parameter value V_i; S_i — the degree of criticality of negative consequences of implementing risk, which decreasing the value of i^{th} criterion.

The first and the fourth column of security matrix characterize the current state of integrated security. Other columns of the matrix represent the dynamics of the process and allow building a forecast of the future.

In this case, the multiplicative convolution of integrated security integral criterion is a value of:

$$K = \prod_{i=1} K_i^{S_i} .$$

Estimates of S_i can be received by experts. However, in most cases it is difficult to give a direct numerical evaluation of these factors for an expert. Therefore, different ranking methods, during the implementation of which the streamline of criteria is only required, may be used preferably.

It can be used, for example, non-strict ranking method. In accordance with this method, the expert makes the numbering of all the criteria descending degree of acceptability of the negative consequences associated with the safety criterion. Moreover, it is assumed that the expert will not be able to distinguish between a certain criteria. In this case, during the ranking he puts them together in random order. Then ranked criteria are consecutively numbered. The rank of criterion is determined by its number.

If in one place there are several criteria, which are indistinguishable among themselves, generally, the evaluation of each of them shall be equal to the average of their new numbers. However, it seems appropriate to modify such valuation method, taking the rank of each of the criteria for the number of indistinguishable entire group as a whole object in the ordering.

In this way, it can be evaluated the degree of influence of each parameter on private safety criteria K_i as well as the degree of acceptability of impacts of threats S_i.

For example, let an expert streamlined criteria as follows:

$$K_5(K_3, K_7, K_2), K_1(K_6, K_8), K_9, K_4.$$

The criteria, which are not distinguishable between themselves are combined in parentheses.

Then the scores for each of the criteria assessed in accordance with the procedure described above, are:

$$S_5 = 1; S_3 = S_7 = S_2 = 2; S_1 = 3;$$

$$S_6 = S_8 = 4; S_9 = 5; S_4 = 6.$$

Let's apply a valuation on the value equal to the sum of all the evaluations:

$$R = \prod_i S_i .$$

In this case R = 29. Thus, after conversion to linear scale [0, 1] to R rate, we will obtain:

$$S_5 = 1/29; S_3 = S_7 = S_2 = 2/29; S_1 = 3/29;$$

$$S_6 = S_8 = 4/29; S_9 = 5/29; S_4 = 6/29.$$

Assessments, which were found with the proposed method are a generalization of Fishburne system of weights for the case of a mixed distribution of preferences, when along with the preferences, the ratios of indifference are included in the system.

Criteria can be grouped in the relevant areas of security in the security matrix, such as: economic, environmental, social, technical, etc.

Thus, each tuple $(K_i, F_i, V_i, S_i, T_i)$ characterizes the state of security on the i - th criterion.

Partial matrix consisting of lines representing a certain direction of safety insurance, describe the condition in the certain field.

K_i safety indicators are closely linked to the consequences of the possible implementation of the existing threats in the system, measures of preventing of such consequences and measures of localization and eliminating of the consequences, if any do arise. It should be emphasized that threats can be divided into primary and secondary. Primary threats exist regardless of the state of the system and have a certain unconditional probability of occurrence. The probability of occurrence of secondary threat is conditional and depends on the state of the system and the state of the environment.

In particular, some of the system can provoke threats, the occurrence of which in other circumstances would have been impossible.

Let's introduce the following notation:

$\overline{UG_i}$ and $\widetilde{UG_j}(i, j = 1,2,3,...)$ — a set of primary and secondary threats arising with probabilities $\overline{PUG_i}$ and $\widetilde{PUG_j}$, and have an influence $\overline{n_{km}}$ and $\widetilde{n_{km}}$ on element (k, m) of matrix B(k = 1,2,3,...; m = 1,2,3,4,5).

The influence of each of the primary or secondary threats can be described as an influence matrix (IM):

$$N_i = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} & n_{15} \\ n_{21} & n_{22} & n_{23} & n_{24} & n_{25} \\ -- & -- & -- & -- & -- \\ n_{n1} & n_{n2} & n_{n3} & n_{n4} & n_{n5} \end{pmatrix}$$

It should be noted that the influence $\overline{n_{km}}$ and $\widetilde{n_{km}}$ on some elements of security matrix B can be either negative or positive.

Elements of influence matrix, that have negative influence, are said to be negative regarding elements of SM. Elements that have a positive influence — positive elements regarding elements of SM. Elements that have no influence, are said to be neutral $\overline{R_i} = \left\{\overline{N_i}; \overline{PUG_i}\right\}$ is said to be execution risk of the i^{th} primary threat.

This reflects the emergence of a tuple with probability $\overline{PUG_i}$ effects that change state of the system through the appropriate influence matrix $\overline{N_i}$.

The probabilities of occurrence of the primary threats. $\overline{PUG_i}$ are not depend from us. However, a set of preventive measures allows to weaken the influence of the primary threats to the level of system security.

It is necessary to analyze the main threats of security of telecommunication systems. They can be divided into two categories: primary and secondary.

The occurrences of the primary threats are independent from us. However, a set of preventive measures of protection allows weakening the influence of the primary threats to the security level of the system [11]. This fact can be described by a matrix of preventive measures (MPM):

$$Z_j = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ -- & -- & -- & -- & -- \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix}$$

where $j = 1...M$, M – total number of preventive measures.

If, despite the preventive protection measures, the implementation of a set of primary threats resulted in consequences, it is necessary to take measures for their localization and elimination.

These measures can be formalized by a matrix of elimination of the consequences (MEC):

$$L = \begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ l_{21} & l_{22} & l_{23} & l_{24} & l_{25} \\ -- & -- & -- & -- & -- \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix}$$

We begin to deal with the primary threats before they attack. In the case of secondary threats we have to prevent them, and that is to deal with the reasons that cause them. This is the fundamental difference in units of measures whose effect is formalized by the set of matrices Z_j and matrix L.

In constructing of fuzzy cognitive model (FCM) the object of study is represented as a semantic-oriented graph [12]. As such models in the

evaluation of integrated security system (ISS) may be adopted:

$$KBS =< G, QL, E > .$$

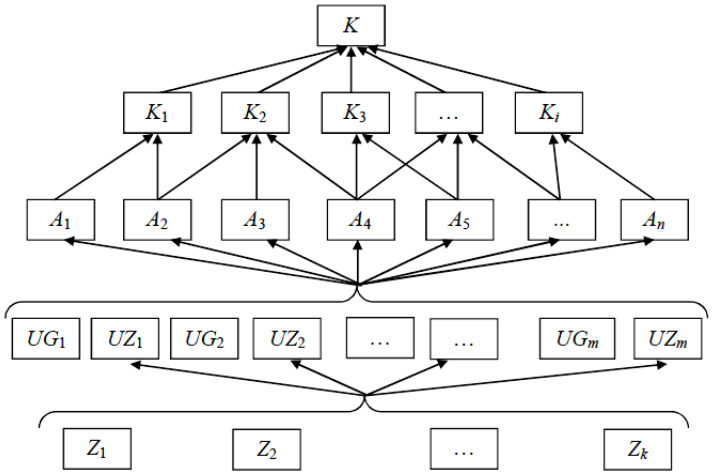
G — oriented graph that has one root apex and contains no loop sand horizontal edges with in the same hierarchy level:

$$G =< \{GF_i\}; \{GD_{ij}\} >$$

where $\{GF_i\}$ — set of root apexes (factors or concepts in terms of FCM); $\{GD_{ij}\}$ – the set of arcs, connecting i^{th} and j^{th} apexes (the set of causal relationships between concepts, with the arc arranged so that the beginning of the arc corresponds to the top of the lower level of the hierarchy (rank) and the end of the arc is the top rank in lesser level); $GF_0 = K$ –root apex, which corresponds to the level of integrated security in general (integral security criterion — target concept); QL–a set of qualitative assessments of levels of each factor in the hierarchy; E – the system of relationships some advantages over other factors according to their impact on a given element.

A generalized example of a graph for a comprehensive assessment of the security of telecommunication system is presented in Figure.

$Z\{1,2,3,...\}$ — are preventive measures of protection (security mechanisms), designed to reduce vulnerabilities of telecommunication system — $UZ\{1,2,3,...\}$, $UG\{1,2,3,...\}$ — are threats to the security of the system, $A\{1,2,3,...\}$ — attacks on telecommunication system, $K\{1,2,3,...\}$ — individual safety performance indicators at the appropriate criteria, K — comprehensive (integral) Index of telecommunication system security.



Impact of factors on the level of integrated security

It should be noted that this connected graph is not a tree, since it does not meet the requirement of absence of simple cycles. This is because the factors in the lowest level of the hierarchy, may simultaneously affect several factors of higher level.

For example, the use of preventive security measures to protect against a vulnerability can simultaneously remove any other vulnerability or lead to a new one.

Some attacks can cause a change of several individual security criteria (sometimes in the opposite direction).

The general algorithm of analysis and integrated security management, based on fuzzy cognitive modeling, can be represented as follows:

1. Gathering of information about the object of protection: identification of assets and the establishment of an entry-level security. In the process of identification the main characteristics of assets should be considered: information value, sensitivity to threats, the availability of protective measures. It is necessary to consider that among the factors that affect the safety, the subjective factors, that are the least predictable, occupy a special place.

2. Selection of criteria, which are characterizing the state of various aspects of security, the definition of its acceptable level.

3. Building a cognitive model as a semantic-oriented graph.

4. Calculation and analysis of integrated security level (ISL) of the systems.

5. If ISL is not in the acceptable range of values, then the changes in the concepts involved in building cognitive models should be made. In aspect of relationships between concepts, their values are being changed through the introduction of protective measures.

Thus, the providing of system security provides a solution to two interrelated problems: the direct problem (analysis of system state) and the inverse problem of management (impact on the system).

In addressing the first problem you need to determine the value of protection criteria K_i and integral criterion K for given values of concepts that affect them.

If the values are outside the range of acceptability, then the solution of the inverse problem must choose such control actions of Z_j and L that will provide a return of target criteria in a safe range.

If there is no single set of necessary control actions, at this stage might appear an optimization problem, consisting in finding such combination of Z_j and L, that provides maximum exposure to negative factors in the set or minimal cost for the implementation of methods of protection.

Conclusions

As a result of research:

1. The security matrix was formed, in which indicators of protection, trends and rate of change and the degree of criticality of negative consequences were selected.

2. The set of preventive measures of protection was defined, that allows weakening of the influence of the primary threats to the security of the system.

3. The implementation of preventive measures was formalized, based on the MEC.

4. The algorithm of analysis and management of integrated security systems, based on cognitive modeling, was developed.

Information security management is greatly simplified and formalized using the fuzzy cognitive modeling. Using this approach contributes to solving problems related to the subjective side in the analysis of information risks and threats. The algorithm allows unifying of approaches to managing of integrated security and beginning of developing of appropriate computational procedures and modules, which can be further used for constructing of telecommunication security systems.

REFERENCES

1. **Haydamakin N**. Concurrent access to information in computer systems — E. : Ural, 2003. — 328 p.

2. **Zegjda D**. Fundamentals of Information System's Security. — M. :Telecom, 2000. — 286 p.

3. **Devianin P.** Computer systems security models — M. : Akademia, 2005. — 144 p.

4. **Kort S**. Theoretical fundamentals of information security. — M. :Gelios, 2004. — 240 p.

5. **Kurilo A.** Information security audit. — M. : BDC-press, 2006. — 304 p.

6. **SaderdinovA**. Information security/ — M. : Dashkovka, 2005. — 336 p.

7. **Petrenko S.** Information Risk Management. Economically justified security. — M. :Press, 2005. — 384 p.

8. **Borisov V**. Fuzzy models and networks. — M. :Telecom, 2007. — 284 p.

9. **Raykov A**. Intelligent Information Technologies. — M. :.MGIREA, 2000. — 96 p.

10. **Vasiliev V.** Analysis and management of information security of colleges on the basis of cognitive modeling. — 2007. — № 1, T. 27. — P. 74–81.

11. **Ajmuhamedov I**. Management of information security in the region based on cognitive modeling. — 2010. — № 1. — P. 96–102.

12. **Ajmuhamedov I.** Modeling based on expert judgments of the evaluation process of information security. — 2009. — № 2. — P. 101–109.

Козловський В. В., Іванов О. В., Сніжко В. В.

АНАЛІЗ ТА УПРАВЛІННЯ БЕЗПЕКОЮ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

У даній статті аналізуються особливості забезпечення захисту інформації, приймаючи до уваги суб'єктивну сторону даного процесу. Основною метою дослідження є розробка алгоритму аналізу та управління комплексною безпекою, котрий дозволить уніфікувати підходи до управління інформаційною безпекою. Безпека не існує сама по собі, у відриві від людини. Вона забезпечується для людини і нею ж оцінюється. Тому, поняття безпеки має не тільки об'єктивну, але й суб'єктивну сторону, оскільки оцінка її рівня проводиться в кінцевому підсумку людиною. Використання методів когнітивного моделювання дозволяє значно покращити процеси аналізу та управління безпекою телекомунікаційної системи. Переваги когнітивного підходу полягають у можливості моделювання слабоструктурованих (тих, що погано формалізуються) систем, які характеризуються неповнотою або невизначеністю знань про них. Застосування розробленого алгоритму дозволить фахівцям приступити до розробки відповідних обчислювальних процедур і модулів, які можуть бути в подальшому використовуватися при забезпеченні захисту телекомунікаційної системи. Результати досліджень будуть також корисні службам, які займаються забезпеченням інформаційної безпеки.

Ключові слова: інформаційна безпека, комплексна безпека, когнітивне моделювання, телекомунікаційна система.

Козловский В. В., Иванов А. В., Снижко В. В.

АНАЛИЗ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

В данной статье анализируются особенности обеспечения защиты информации, принимая во внимание субъективную сторону данного процесса. Основной целью исследования является разработка алгоритма анализа и управления комплексной безопасностью, который позволит унифицировать подходы к управлению информационной безопасностью. Безопасность не существует сама по себе, в отрыве от человека. Она обеспечивается для человека и им же оценивается. Поэтому, понятие безопасности имеет не только объективную, но и субъективную сторону, поскольку оценка ее уровня проводится в конечном итоге человеком. Использование методов когнитивного моделирования позволяет значительно улучшить процессы анализа и управления безопасностью телекоммуникационной системы. Преимущества когнитивного подхода заключаются в возможности моделирования слабоструктурированных (тех, что плохо формализуются) систем, которые характеризуются неполнотой или неопределенностью знаний о них. Применение разработанного алгоритма позволит специалистам приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использоваться при обеспечении защиты телекоммуникационной системы. Результаты исследований будут также полезны службам, которые занимаются обеспечением информационной безопасности.

Ключевые слова: информационная безопасность, комплексная безопасность, когнитивное моделирование, телекоммуникационная система.

Kozlovskii V. V., Ivanov O. V., Snizhko V. V.

ANALYSIS AND SECURITY MANAGEMENT OF TELECOMMUNICATION SYSTEMS BASED ON PREDICTIVE TECHNOLOGIES

This paper presents the peculiarities of providing information, taking into account the subjective aspect of this process. The main purpose of the study is to develop an algorithm for analyzing and managing integrated security, which will unify the approaches to information security management. Security does not exist by itself, in isolation from a person. It is provided for a person and it is appreciated. Therefore, the notion of security has not only an objective but also a subjective aspect, since the assessment of its level is ultimately man. Using cognitive modeling methods can greatly improve the analysis and management of the security of the telecommunication system. The advantages of the cognitive approach are the ability to simulate poorly structured (poorly formalized) systems that are characterized by incomplete or uncertain knowledge of them. The application of the developed algorithm will allow the specialists to begin to develop appropriate computational procedures and modules, which can be further used in telecommunication system security. The results of the research will be useful for information security specialists.

Keywords: information security, integrated security, cognitive modeling, telecommunication system.

Стаття надійшла до редакції 05.09.2018 р.
Прийнято до друку 18.09.2018 р.
Рецензент – д-р техн. наук, проф. Мачалін І. О.