UDC 629.73:681.51 (045)
DOI: 10.18372/2306-1472.79.13828

Oleh Alexeiev [1]
Viktoriia Volkogon [2]
Ruslan Pechevystyi [3]
Serob Karapetian [4]

ANALYSIS OF WORLD STANDARDS OF RISK MANAGEMENT IN THE CONTEXT OF IMPLEMENTATION OF AVIATION ACTIVITY

National Aviation University, 1, Kosmonavta Komarova ave., Kyiv, 03058, Ukraine
E-mails: [1]oalexeiev@yahoo.com; [2]sonechkovikaa@gmail.com; [3]rick999@ukr.net;
[4]serobkarapetyan@gmail.com

Abstract

The article deals with the analysis of world standards of risk management. It is determined that due to the similarity of the nature of the risks, the relevance of their reduction to the minimum possible level has increased. The creation of the latest methodology for controlling the level of flight safety, for providing and supporting decision-making by the human operator, provides for the critical elements of the ATM system to control the level of risk.

Keywords: risks; aviation activity; safety management system; risk management

1. Introduction

Over the past decade, air traffic controller activity has taken place in conditions of uncertainty and instability of factors of the external and internal environment, which increases the probability of occurrence of various and significant risks. Speaking of risks, the first is the ability to incur some loss (loss, damage) with a certain probability [1, 2]. Because of the influence of risk factors, financial, material, labor, time and other specific types of losses are possible [3].

Often, airlines are concerned with the uncertainty of the external and internal environment that generates risks. Thus, according to the theory of statistics, "risk is the probability of occurrence of an event, which may entail a deviation from the expected trend" [3-5]. From the point of view of the impact on the efficiency of the commercial operations "risk - the possibility of unforeseen damage from the incident, which completely modifies the initial conditions for the flight" [5, 6].

2. Analysis of the latest research and publications

In [7-9], risk is defined as "an effect that can lead to losses or other losses." The international PMBOK standard defines the project risk as a "set of elements in the project management, including identification, analysis and response processes to the risks arising in the project". In [10], risk is treated as "the level of losses that are expressed in the ability not to achieve the objective; b) uncertainty of the expected result; c) in the subjectivity of the estimation of the predicted result. In [11] states that risk management is a means of preventing or reducing adverse impacts on the results of long-term forecasting and strategic planning, the development of a well-founded concept and development programs adapted to uncertainty. In [11], the risk management process is considered as one of the elements of a management system that represents the preparation and implementation of measures that reduce the consequences of making erroneous decisions and reduce the possible negative effects of unwanted events that may arise during the implementation of the adopted RM (risk management) . In [8], risk management is defined as a process that balances the enterprise's various resources to achieve its purposes using technological, organizational and financial tools. Some scientists define "risk management" as a complex of managerial decisions aimed at reducing the likelihood of adverse outcomes in the enterprise and reducing possible losses from their implementation [5-8].

3. Theoretical part

Dangers include various technical malfunctions and crashes, as well as contradictory data in information systems, as well as unlimited access of staff to corporate information. In order to achieve the high

efficiency of RMS (risk management system), international standards (ISO 15408, ISO 17799 (BS7799), ISO 27000 series, developed and widely used to date), various standards of national providers BSI (Great Britain), NIST 80030 (USA), SAC (PRC), other normative and reference libraries and standards (COSO, ITIL, SAS 55/78).

Standard ISO 17799 (in 2005 the standard has been redone, supplemented and published as ISO / IEC 27002) uses a broader risk treatment as combining the likelihood of an adverse event and the consequences of its occurrence. The ISO 27005 standard specifies the term "information risk", distinguishing its components, threats, vulnerabilities and losses. So, according to ISO 27005: "Information security risk is a potential use of the vulnerability of an asset or group of assets for a specific threat to harm the organization" [3]. At the same time, from the standpoint of a systematic approach to analyzing the problem of information security of an enterprise, there is a need for a deeper classification of aviation risks. International standards, in addition to describing the minimum necessary set of mechanisms and tools for achieving and maintaining security, include requirements for evaluation of risks and calculating the cost-effectiveness of using different mechanisms for their management.

In order to manage information risks, particular methods have been developed. Those methods are described in international, national and other standards and documents (ISO 15408, ISO 17799 (BS7799), a series of standards ISO 27000; BSI, NIST 80030, SAC, COSO, SAS 55/78). Summarizing the methods and tools described in them, risk management includes the following steps [1]:

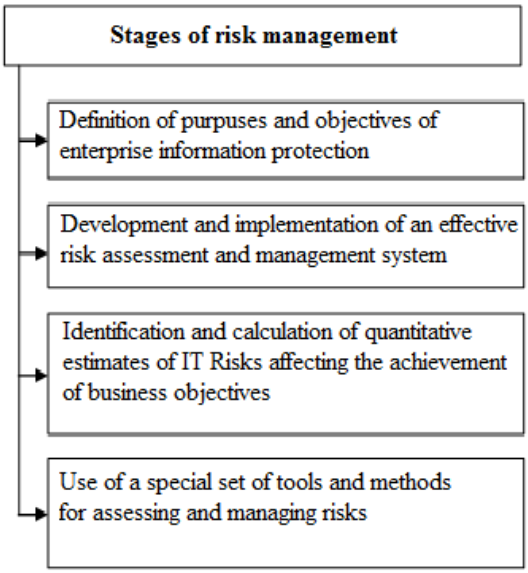

Fig. 1. Stages of risk management

Let's take a look at some of the international security standards. In 2005, the new BS 7799 Standard Part 3 was developed in the UK. "Information Security Management Systems - Practical Rules for Information Security Risk Management" [11]. In the following, it was redefined and transferred to the International Organization for Standardization (ISO and IES). Currently, the standard is approved as ISO IEC20071.

Based on the provisions of the British BS standards, a series of ISO / IEC 27000 standards, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), was developed. International standards ISO 27002 and ISO 27001 are among the most widely used in the field of information security. ISO 27002 (formerly ISO 17799) includes a description of the main recommendations for the organization of effective security management systems, removing the attention of all key aspects [1, 2].

The ISO 27001 information security standard is a collection of criteria used for system analysis and evaluation management, the results of which an accredited center issues a certificate of compliance, which is entered into the register. The ISO 27001 standard describes a security management system aimed at solving the tasks of developing and implementing enterprise security enhancements, which uses a cycle consisting of development, analysis and review. This cycle is widely known as the PDCA Plan-Do-Check-Act model, which is shown in Fig. 2.

In 2012, the International Association for the Audit and Control of Information Systems Basa introduced an updated version of the COBIT5 (Control Objectives for Information and Related Technologies) standard. COBIT provides an implementable set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers. This standard includes best practices in management and strategic IT governance.

The COBIT5 includes 5 principles (Fig.3) that allow taking into account the seven factors influencing effective management and management that provide optimization of investment in information technology [7]. These principles form the motive and potential for practical risk management activities.

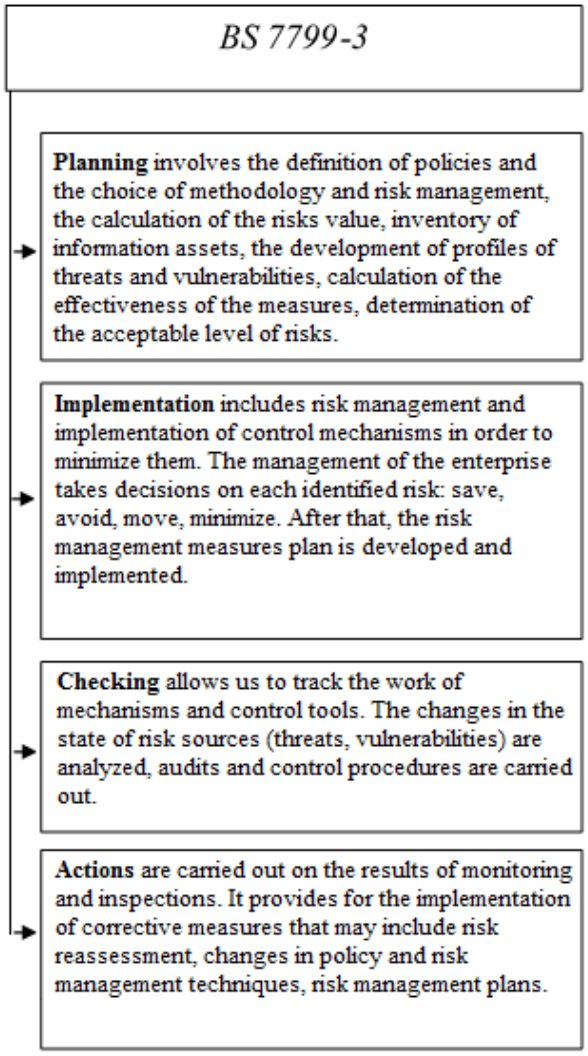

Fig. 2. PDCA model

However, existing standards in the area of information security and risk (ISO 15408, ISO 17799, ISO 9001, NIST 800-30, BSI, BS 7799, COBIT, ITIL, etc.) do not regard a number of fundamental issues that need to be considered when developing management techniques risks. The list of these issues is determined by the level of development of the enterprise, the specifics of its activities and other parameters. Consequently, it is impossible to develop a single, suitable for all domestic enterprises risk management methodology that would allow for economically sound security. In each case, it is advisable to adapt it to the needs of a particular company, taking into account the specific conditions for its functioning.

In practice, there are no unconditional rules that fix, in which case it is advisable to use one or another methodology of information risk management. Most of them are based on international standards, such as BS7799 or IS017799, and therefore they can not assess the size of IT risks at the enterprise and the standard that is being used.

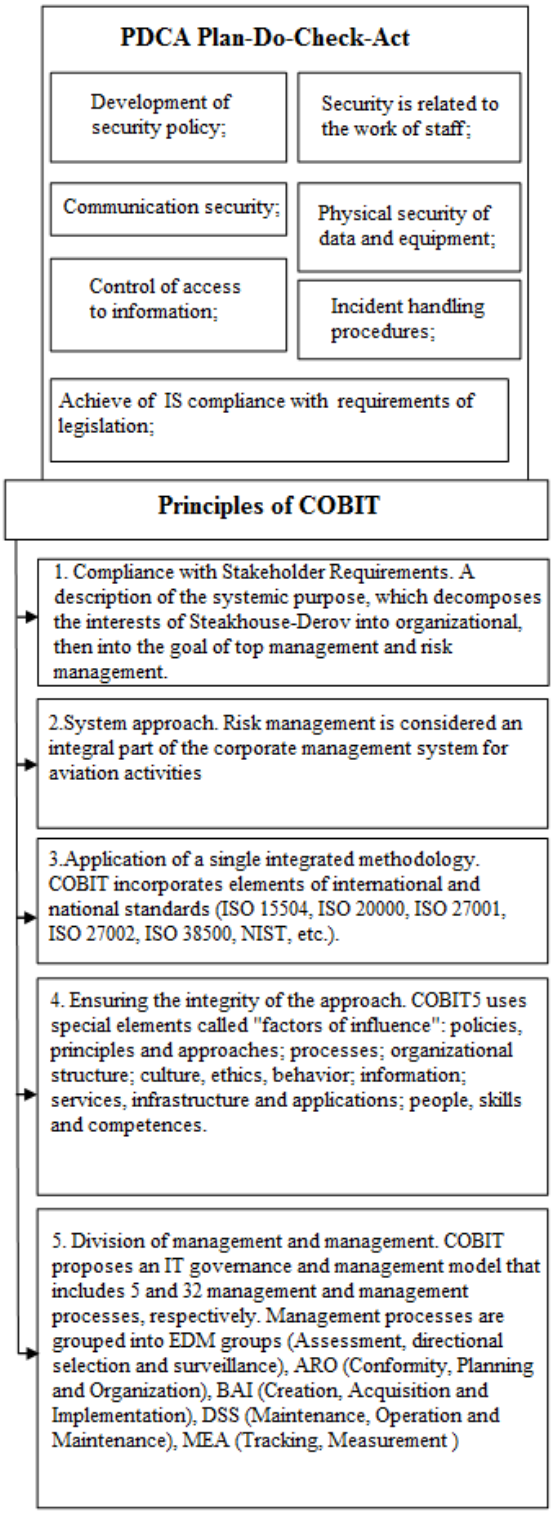

Fig. 3. Principles of COBIT

The growing dependence of production processes on information technologies in many respects causes an increase in the relevance of issues of environmental and industrial safety. In connection with this, there is a need for the adoption of RM, aimed at increasing the level of information security, since each year the number of accidents occurring through the fault of information systems is only increasing.

The most complex and heterogeneous process is risk assessment, the only methodology that does not exist. In order to regulate the processes for assessing all types of risks in 2009, ISO 31010 "Risk Assessment Methods" was implemented. According to it, risk assessment is a process that includes identification, analysis and comparative risk assessment [33, 48].

The risk analysis consists of the steps outlined in the following sections. Methods used in risk analysis are divided into qualitative, quantitative or mixed. The qualitative assessment describes the consequences of the risks, their probability and magnitude on the scale "high", "medium" and "low"; comparative risk assessment in this case is carried out on the basis of qualitative criteria.

When quantitative analysis of risks is determined by the significance and monetary value of the consequences of their probability of occurrence, while the risk value is obtained in - units given in the development of the scope of risk management. A full quantitative risk analysis is not always carried out due to the incompleteness of available data, the analyzed system, and because of the significant impact of the human factor.

A comparative risk assessment involves comparing the quantitative risk value with the criteria set for determining the scope of risk management to determine the risk category and significance.

ISO 31010 describes the main methods used for risk assessment, taking into account their possible application at different stages of the assessment procedure, including: brainstorming method, Delphi method, checklist, hazard analysis and critical control points, scenario analysis, analysis of the failure tree, analysis of causes and consequences, decision tree analysis, Markov analysis, Monte Carlo simulation, Bayesian analysis and Bayesian network, FN curves, risk indices, matrix of consequences and probabilities, multicriteria analysis decisions.

The assessment of risks involves not only the assessment of the likelihood of occurrence of risk events, but also the determination of the amount of damage in the event of these events. It should take into account both direct and indirect losses. Direct losses represent a direct loss to the health of third parties, property or property interests of the enterprise (third parties). Indirect damage arises due to the impossibility of normal functioning of the enterprise for a certain time.

Despite all the advantages, it should be noted that the significant disadvantage of these standards is the lack of a methodological basis for an integrated analysis of various risk factors (qualitative and quantitative) [9].

Thus, we must recognize that formalization and automation are needed at different stages to improve the effectiveness of risk management. Such a task can be solved by developing a decision support system (DSS), risk management. DSS should be based on modern methods of processing information in conditions of significant uncertainty and allow to carry out risk analysis, produce, evaluate and make effective decisions. To this end, the system should use models that integrate qualitative and quantitative factors that determine aviation risks [11].

4. Conclusions

Due to the similarity of the nature of the appearance of risks and the relevance of their reduction increased to an acceptable level. For various critical parts of the system - reducing the level of risk makes it urgent to create a methodology to ensure and maintain a guaranteed level of safety of future flights.

For various critical parts of the system - reducing the level of risk makes it urgent to create a methodology to ensure and maintain a guaranteed level of safety of future flights. The purpose of the methodology is to integrate into a single set of tasks the assessment, provision and verification of the security of aviation, as a complex hierarchical structure with independent critical elements, as well as hardware, software, network and ergo components, which are both a means and an object of safety [3,4,8].

Implementation of the guaranteed result is to implement the management processes in such a way as to prevent the transition of the infrastructure or its systems to a potentially hazardous state. Besides to ensure the blocking (exception) of the relevant technical object in the event of a threat of transition or when the transition to a dangerous state and minimization of the consequences of such a transition.

References

[1] Kharchenko V., Alexeiev O., Kolesnyk T. (2018) Ensuring the guaranteed level of flights

safety – the view of the future. *Proceedings of the National Aviation University*, №4(77).

[2] Kharchenko V., Alexeiev, Babeichuk D. (2010) Method analysis of management decisions making while air navigation functioning in emergency situations. *Proceedings of the National Aviation University*. – K. – 86p.

[3] Kojohina O., Alexeiev O., Blahaja L., Rudass S. (2016) Information Reliability of radar. *System Operator Science journal*. Poland

[4] Alexeiev O.M., Luppo O.E., Kolesnyk T.A. (2017) Importance of the single european sky performance scheme implementation. *Norwegian journal of development of the international science*, no. 2, Vol.1

[5] Kharchenko V., Alexeiev O., Yrchik R., Ali I. (2017) Some aspects of municipal aviation functioning. *Proceeding of the National Aviation University*. (no.2(71)

[6] Kharchenko V., Alexeiev O., Rudas S., Kozhokhina O. (2017) Application of imprecise models in analysis of risk management of software systems. *Proceedings of the National Aviation University*. №2(71).

[7] Puzyrev A., Alexeiev O., Leftor V (2017) Monitoring device for operating climatic conductions light aircraft. *Electronic and control systems, no* 1(51)

[8] Alexeiev O.M, Bondarev D.I., Shmeleva T.F., Sedina A.I. (2016) Ummanned Aircraft Usage in the Municipal Air Transport of Ukraine. *Proceedings The seventh world congress "Aviation in the XXI-st century" Safety in aviation and Spase Technologies*. Kyiv

[9] Kharchenko V.P., Alexeiev O.M. (2016) General principles of decision – making support in provision of guaranteed level of safety. *Proceeding of the seventh world congress "Aviation in the XXI-st century" Safety in aviation and Spase Technologies*. Kyiv

[10] Puzyrev A., Alexeiev O., Ushakov V., Volkogon V. (2017) Development of airframe design elements control technique under operational conditions. *Electronic and control systems*, no. 2(50)

[11] Kharchenko V., Alexeiev O., Tapia K. (2013) Collision probability of aircraft flying on parallel track. *Proceedings of the National Aviation University*.– K.– 86p.

О. М. Алєксєєв[1], В. О. Волкогон[2], Р. П. Печевистий[3], С. С. Карапетян[4]

Аналіз світових стандартів управління ризиками в контексті здійснення авіаційної діяльності

Національний авіаційний університет, просп. Космонавта Комарова, 1, Київ, Україна, 03058
E-mails: [1]oalexeiev@yahoo.com; [2]sonechkovikaa@gmail.com; rick999@ukr.net; serobkarapetyan@gmail.com

У статті розглянуто аналіз світових стандартів управління ризиками. Так визначено, що схожість природи появи ризиків зросла актуальність їх зниження до прийнятного рівня для різних критичних додатків обумовлює актуальність створення методології забезпечення і підтримки гарантованого рівня безпеки майбутніх польотів.

Ключові слова: ризики; авіаційна діяльність; управління безпекою польотів; управління ризиками

О. Н. Алексеев[1], В. А. Волкогон[2], Р. П. Печевистый[3], С. С. Карапетян[4]

Анализ мировых стандартов управления рисками в контексте осуществления авиационной деятельности

Национальный авиационный университет, просп. Космонавта Комарова, 1, Киев, Украина, 03058
E-mails: [1]oalexeiev@yahoo.com; [2]sonechkovikaa@gmail.com; [3]rick999@ukr.net; [4]serobkarapetyan@gmail.com

В статье рассмотрен анализ мировых стандартов управления рисками. Так определено, что сходство природы появления рисков возросла актуальность их снижения до приемлемого уровня для различных критических приложений обусловливает актуальность создания методологии обеспечения и поддержания гарантированного уровня безопасности будущих полетов.

Ключевые слова: риски; авиационная деятельность; управление безопасностью полетов ; управление рисками

Alexeiev Oleh. (1978). Candidate of Technical Sciences.
Associate Professor of Air Navigation Systems department of Institute of Air navigation in National Aviation University, doctoral student.
Education: Faculty of Air Traffic Services, State Flight Academy of Ukraine, Kirovograd, Ukraine (2000).
Research area: improvement and automation of a professional selection system and development of professional-major.
Publications: 41.
E-mail: oalexeiev@yahoo.com

Viktoriia Volkogon. Applicant at the Department of Air Navigation Systems, National Aviation University, Kyiv, Ukraine.
Education: Institute of Air Navigation Services, National Aviation University (2013).
Research area: free flight aircraft and resolution of conflict situations in a free flight.
Publications: 18.
E-mail: sonechkovikaa@gmail.com

Ruslan Pechevystyi. Postgraduate student in Aviation Transport of National Aviation University.
Air traffic control officer. ACC unit. Kyivcenteraero. UkSATSE
Research area: Decision making, Flight Safety Management, prevention and investigation of aviation events and incidents. Publications: 2
E-mail: rick999@ukr.net

Serob Karapetyan. Postgraduate student in Aviation Transport of National Aviation University. Kyiv, Ukraine.
Education: Institute of Air Navigation Services, National Aviation University (1986).
Research area: free flight aircraft and resolution of conflict situations in a free flight.
Publications: 1.
E-mail: serobkarapetyan@gmail.com