UDC 004.056.345

O.A. Zamula[1], V.I. Chernysh[1], O.V. Sievierinov[2]

[1]*Kharkiv national university of radioelectronics, Kharkiv*
[2]*Kozhedub Air Force university, Kharkiv*

IMPLEMENTATION INTERNATIONAL STANDARDS IN THE UKRAINIAN AIR TRAFFIC MANAGEMENT SYSTEM

In the article we can find the analysis EUROCONTROL Safety Regulatory Requirement and international standard called ISO/IEC 27001:2005. Moreover, the main statements, terms, were conceptualize. They are connected with the safety software in procedures of air traffic management, particularly air traffic control equipment. Finally, in the article requirements were analyzed and they were able to implement in the Ukrainian air traffic service enterprise.

Keywords: *information security, risk, standard, threat, air traffic management.*

The first thing that needs to be consider is that the main problem for information security in air traffic management (ATM) system is opportunity of unauthorized access in the procedures of air traffic control (ATC). As we know modern ATM systems have a lot of different vulnerabilities. Therefore, we must consider two issues:

1) the security operation of ATM systems under normal operating conditions;

2) the protection of ATM systems in an increasingly aggressive environment.

Moreover, we must consider the tasks of information security in ATM as the part of aviation security. Nowadays, the information security is the most important question in information technology (IT). It's no wonder that modern IT are spread in ATM systems.

Information technology [1; 2, p. 20] – the technology of the production, storage, and communication of information using computers and microelectronics.

The purpose of the work is analysis of international standards and requirements, particularly EUROCONTROL SAFETY REGULATORY REQUIREMENT (ESARR) and international standard in information security management called *ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements. Furthermore*, in this article authors are considering practical issues for implementing these standards in the Ukrainian air traffic management system.

Introduction

The Air Transportation System is a classic example of what has become known as a “System of Systems”. It is an evolved complex system with subsystems. These subsystems include technical, operational, organizational and social components. For the analysis of this paperwork the Air Transportation System will be parsed into several interacting subsystems (fig. 1):

1) the Air Traffic Management System;

2) the Vehicle System (Including the Pilot);

3) the Airline System.

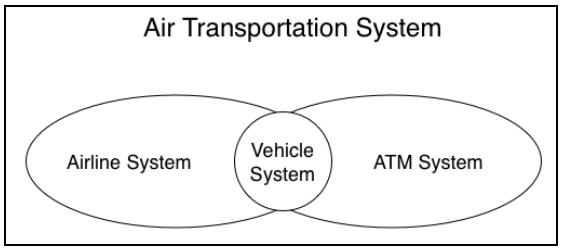

Fig. 1. General structure of Air Transportation System

The Vehicle System is the smallest operational system element in this decomposition. The control of the vehicle and its subsystems constitute the inner loop of the air transportation system. The vehicle is a joint element of Airline and the Air Traffic Management subsystems which interact operationally through joint control of the vehicles they are responsible for. The Airline System also includes a business component that involves scheduling and pricing. All of these subsystems are part of a macro loop that defines the response of the overall Air Transportation System to demand and other social, technical and operational drivers.

One of the main tasks of the ATM system is to ensure the sustainability of IT products. The vast majority of facilities, which cover information security tasks is unidirectionality. In addition to this, they are being considered as a one-time task. However, we should take into account that modern IT are developed and improved. According to this tendency, security techniques must be enhanced and IT staff must hone their skills in the sphere of information security. Another problem that we should consider is evolution of threats in ATM information systems.

In order to avoid such situations, the information security should be perceived as a "continuous process", which integrated into the corporate management model company. But, the majority of branch-wise standards

doesn't have requirements for protecting critical ATM information systems. Therefore, the main necessity for ATM systems is implementation ESARR with international standards in information security management (e.g. ISO/IEC 27001:2005) [2, 3].

Analysis of EUROCONTROL safety regulatory requirements

The main characteristic that defines the operational efficiency of the ATM system is safety. For achieving the target level of ICAO safety, the air-navigation providers must establish safety requirements for ATM services and ensure their implementation. This mechanism established a Safety Regulation Commission (SRC) as an independent body to the EUROCONTROL Agency. Its purpose is to provide advice and support the achievement of consistent high levels of safety in air traffic management (ATM) within European Civil Aviation Conference (ECAC) area [7 – 11].

The SRC is responsible for:

1) the development and uniform implementation of harmonised safety regulatory objectives;

2) the development of target levels of safety; and,

3) standards of safety performance.

ESARRs are approved by the EUROCONTROL Permanent Commission for implementation by States, national safety regulatory authorities and Air Navigation Service Providers (ANSP). Where necessary, SRC establishes procedures for the uniform national application of ESARRs.

Let's consider the requirements in more detail (fig. 2).

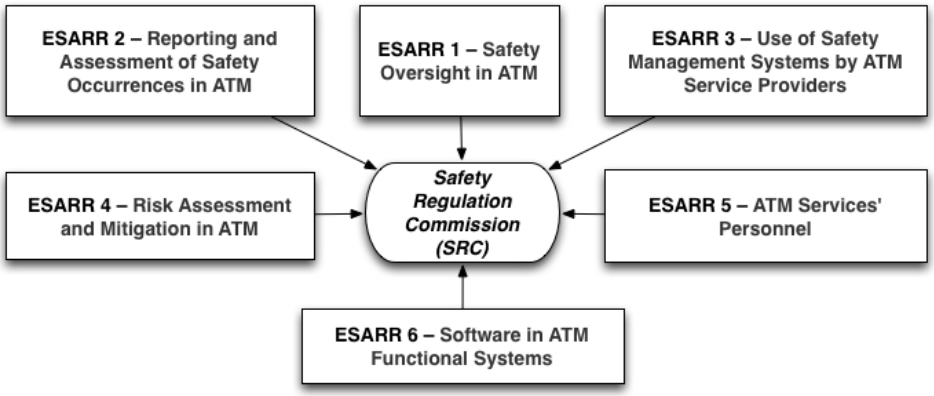

Fig. 2. EUROCONTROL Safety Regulatory Requirements

ESARR1: Safety Oversight in ATM [7, p. 22]. ESARR 1 provides a set of safety regulatory requirements for the implementation of an effective safety oversight function in EUROCONTROL Member States. Its provisions support a process approach to the safety oversight of the ATM service providers and define the minimum elements that must exist in the safety oversight processes deployed by national regulatory authorities.

The requirement addresses the critical elements of the safety oversight process to ensure a robust supervision of safety. The following main processes are required for implementation by national regulatory authorities:

1) regular monitoring and assessment of safety levels achieved by the service providers against the target (tolerable) levels of safety determined for the respective airspace volumes;

2) verification of compliance with the applicable safety regulatory requirements established by the rule making body and other safety related conditions and arrangements needed to implement them;

3) safety regulatory auditing as the means to obtain objective evidence of compliance with the applicable safety regulatory requirements;

4) safety oversight of new systems and changes to the ATM system, which is built around the review of safety arguments proposed by the service providers consistent with the safety regulatory framework in which they operate.

We must note that ESARR 1 addresses the safety oversight processes, their principles and interrelated elements and outputs without identifying the set of applicable safety regulatory requirements which constitute the regulatory reference for verification.

That reference depends on the actual regulatory framework enforced through the specific state regulatory process [7].

ESARR 2: Reporting and Assessment of Safety Occurrences in ATM [8]. This requirement promotes systematic reporting and assessment process, encourages the establishment of a non-punitive environment and is designed to act as an effective contribution to accident and serious risk bearing incident prevention [8].

Moreover, it defines:

1) requirements on the main phases of the occurrence reporting and assessment process:

- occurrence reporting;

- data collection, data analysis, risk classification, recommendation formulation;

- recommendation implementation and monitoring; safety data and experience exchange.

2) the minimum appropriate safety data which shall be collated and reported to EUROCONTROL by States, expressed in terms of high level safety indicators.

3) harmonised and systemized terms, definitions.

ESARR 3: Use of Safety Management System by ATM Service Providers [9]. The requirement mandates the implementation and use of Safety Management Systems (SMS) by providers of ATM services. The main aim of this requirement is to ensure that all safety issues and risks within the provision of the ATM service have been addressed in a satisfactory manner, and to a satisfactory conclusion.

ESARR 4: Risk Assessment and Mitigation in ATM [10]. This requirement concerns the use of a quantitative risk based-approach in ATM when introducing and/or planning changes to the ATM system. It covers the human, procedural and equipment (hardware, software) elements of the ATM system, as well as its environment of operations.

ESARR 4 covers the complete life-cycle of the ATM system, and, in particular, its constituent parts. The assessment of planned and/or implemented organisational or management changes to the ATM service provision are outside the scope of the requirement.

The objective of this requirement is to ensure that the risks associated with hazards in the airborne and ground components of the ATM system are systematically and formally identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated safety regulatory authority.

ESARR 5: ATM Services' Personnel [11]. ESARR 5 sets out the general safety regulatory requirements for all ATM services' personnel responsible for safety related tasks within the provision of ATM services across the ECAC area, as well as specific safety regulatory requirements for air traffic controllers and for engineering and technical personnel undertaking operational safety related tasks. The overall objective of the requirement is to ensure the competency and, where applicable, the satisfaction of medical requirements, of ATM services' personnel responsible for safety related tasks within the provision of ATM services.

ESARR 6: Software in ATM Systems [2]. The requirement concerns the implementation of software assurance systems to ensure that the risks associated with the use of software safety related ground-based ATM systems are reduced to a tolerable level. For this purpose it provides a set of harmonised safety regulatory requirements concerning the ground component of the ATM system, and the ground-based supporting services (including communication, navigation and surveillance systems) under managerial control of the ATM service provider. ESARR 6 is not applicable to the airborne or space components of the of ATM systems.

The requirement does not identify any software assurance standard as an acceptable means of compliance to meet its mandatory provisions. Accordingly, it does not prescribe any type of supporting means of compliance for software.

The provisions of EASRR 6 have been developed on the bases that an a priori effective risk assessment and mitigation process is conducted to an appropriate level to ensure that due consideration is given to all aspects of ATM, including ATM functions to be performed by software.

ESARR 6 requires ATM service providers to implement a software safety assurance system within the framework of their safety management systems to deal specifically with software related risk assessment and mitigation aspects, including all on-line software operational changes.

The software safety assurance system must ensure allocation of software assurance levels to all operational ATM software. These levels relate to the rigour of the software assurance and the safety criticality of the assessed software. A minimum of four software assurance levels are required, with level 1 indicating the most critical level. Software assurance levels are allocated according to the most adverse effect that software malfunctions or failures may cause, as per ESARR 4.

ESARR 6 mandatory provisions include software validation and verification, configuration management and requirements traceability assurances within the scope of the software safety assurance system.

Analysis of regulatory documents [2, 7 – 11] shows that there is no single standard in the management of information security ATM resources. Moreover, ESARR 6 standard does not consider any requirements for the methods, tools and techniques to achieve the necessary level of security ATM software, including to information security ATM. This role must perform national or international standards for information security management, for instance ISO/IEC 27001:2005 "Information technology security practices. Information Security Management System. Requirements".

Analysis of the international standard ISO / IEC 27001:2005

The standard called ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations [2].

ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific

requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified according to the standard.

This standard contains 11 domains (apart from introductory sections):

1) security policy describes management direction;

2) organization of information security describes governance of information security;

3) asset management describes inventory and classification of information assets;

4) human resources security describes security aspects for employees joining, moving and leaving an organization;

5) physical and environmental security describes protection of the computer facilities;

6) communications and operations management describes management of technical security controls in systems and networks;

7) access control describes restriction of access rights to networks, systems, applications, functions and data;

8) information systems acquisition, development and maintenance describes building security into applications;

9) information security incident management describes anticipating and responding appropriately to information security breaches;

10) business continuity management describes protecting, maintaining and recovering business-critical processes and systems;

11) compliance describes ensuring conformance with information security policies, standards, laws and regulations;

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of IT or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole. Moreover business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

1) systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;

2) design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

3) adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Conclusions

Implementation of Information Security Management System using ISO / IEC 27001:2005 allows to organise process approach for information security. This procedure can systemize and solve the problem of information protection in ATM system from external and internal threats.

EUROCONTROL Safety Regulatory Requirements don't cover issues which connected with information security management and risk assessment of information security. However, ESARR 6 demands of software, which use in ATM system.

Finally, if we want to build dependable information system in air traffic management of Ukraine, we must implement ISO/IEC 27001:2005 and ESARR 6 together. In this case, security system will cover all procedures, tools and equipment which provide aviation safety. This approach is effective for realisation Integrated Management System.

References

1. Захист інформації в системі організації повітряного руху / І.С. Биковець, В.О. Клименко, С.Г.Кравцов та ін.. – К.: ДП ОПР України, 2008. – 235 с.

2. ESSAR 6 SOFTWARE IN ATM FUNCTIONAL SYSTEMS – Eurocontrol, 2010 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR6.

3. ISO 27001 ISO/IEC 27001:2005/BS 7799-2:2005 Information technology. Security techniques. Information security management systems. Requirements - ISO / IEC, 2005.

4. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації. – Х.: ХУ ПС, 2011. – Вип. 2 (92). – С. 53-56.

5. Замула А.А. Международные стандарты в области оценивания информационных рисков / А.А. Замула, В.И. Черныш, К.И. Иванов // Технические средства защиты информации: Тез. докл. IX Белорусско–российской НТК, 28-29 июня 2011 г. – Минск : БГУИР, 2011. – С. 9.

6. Замула А.А. Оценивание рисков информационной безопасности в современных информационных системах / А.А. Замула, В.И. Черныш, К.И. Иванов // XIV Межд. НПК «Безопасность информации в информационно – телекоммуникационных системах», тез/ докл. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. – С. 31.

7. ESARR 1 SAFETY OVERSIGHT IN ATM – Eurocontrol, 2009 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR1.

8. ESARR 2 REPORTING AND ASSESSMENT OF SAFETY OCCURRENCES IN ATM – Eurocontrol, 2009 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR2.

9. ESARR 3 USE OF SAFETY MANAGEMENT SYSTEMS BY ATM SERVICE PROVIDERS ATM – Eurocontrol, 2000 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR63.

10. ESARR 4 RISK ASSESSMENT AND MITIGATION IN ATM – Eurocontrol, 2001 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR4.

11. ESARR 5 ATM SERVICES' PERSONNEL– Eurocontrol, 2002 [Electronic resource]. – Attached to: http://www.skybrary.aero/index.php/ESARR5.

12. Сєвєрінов О.В. Управління інформаційною безпекою згідно міжнародних стандартів / О.В. Сєвєрінов , В.І. Черниш // Системи управління,навігації та зв'язку. Збірник наук. праць. Вип. 4(20). – К.: ЦНДІ НіУ, 2011. – С. 250–253.

Надійшла до редколегії 3.09.2014

Рецензент: д-р техн. наук проф. Ю.В. Стасев, Харківський університет Повітряних сил ім. І. Кожедуба, Харків.

ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНИХ СТАНДАРТІВ В СИСТЕМУ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ УКРАЇНИ

О.А. Замула, В.І. Черниш, О.В. Сєвєрінов

У статті проводиться аналіз регулятивних вимог Євроконтролю з безпеки системи організації повітряного руху та міжнародного стандарту ISO / IEC 27001: 2005. Концептуалізовані основні визначення, поняття, терміни, що стосуються забезпечення безпеки програмного забезпечення наземних засобів системи організації повітряного руху. Даються рекомендації з гармонізації та впровадженню даних нормативних документів у Інтегровану систему управління Державного підприємства обслуговування повітряного руху України.

***Ключові слова**: інформаційна безпека, ризик, стандарт, загроза, організація повітряного руху.*

ИМПЛЕМЕНТАЦИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ В СИСТЕМУ ОРГАНИЗАЦИИ ВОЗДУШНОГО ДВИЖЕНИЯ УКРАИНЫ

А.А. Замула, В.И. Черныш, А.В. Северинов

В статье проводится анализ Регулятивных требований Евроконтроля по безопасности системы организации воздушного движения и международного стандарта ISO/IEC 27001:2005. Концептуализированы основные определения, понятия, термины, касающиеся обеспечения безопасности программного обеспечения наземных средств системы организации воздушного движения. Даются рекомендации по гармонизации и внедрению данных нормативных документов в Интегрированную систему управления Государственного предприятия обслуживания воздушного движения Украины.

***Ключевые слова:** информационная безопасность, риск, стандарт, угроза, организация воздушного движения.*