Methods of information systems protection

UDC 004.056 **doi: 10.20998/2522-9052.2020.4.17**

Vladyslav Chernysh

Non-governmental organization "Civil Aviation of Ukraine", Kyiv, Ukraine

MODEL OF FUNCTIONAL HAZARD ASSESSMENT IN AIR TRAFFIC MANAGEMENT SYSTEM REGARDING INFORMATION SECURITY THREATS

Abstract. The threat to information security for the air navigation service providers represents a potential violation of information security of the information infrastructure elements in the air traffic management system such as communications, navigation and surveillance equipment, and the information and telecommunication systems. Typically, a threat results from the presence of vulnerable components in the protection of information technology as part of air navigation service providers' activity. Most of the approaches and techniques of international aviation organizations and best-practices of air navigation service providers are focused on developing risk methods and models regarding aviation safety. A well-known problem with aviation safety risk assessment is that it does not take into account the information and cyber security threats. **The subject** of the article is exploration of methods and models for risk assessment of air navigation service providers. **The purpose** is the development of model of functional hazard assessment and set of information security requirements for air navigation service providers. The proposed model of functional hazard assessment differs from the known by detailing of information security sphere. The software model of functional hazard assessment was developed via MATLAB Fuzzy Logic Toolbox. **Practical significance** is that the obtained results allow air navigation service providers to make better decisions regarding management systems maturity improvement.

Keywords: air navigation service provider; air traffic service; risk; safety; air traffic management; information security; threats.

Introduction

The first thing that needs to be said is that the activities of the air navigation service provider (ANSP) are organized using information and telecommunication systems (ITS) for the realization of operation activity – core processes.

Awareness of the problem of air traffic management (ATM) infrastructure security risk management has led ANSP to define risk management strategies for aviation safety, ATM security (including cyber and information security), occupational safety, etc.

Prevention of aviation accidents and incidents related to operational activities in the provision of air navigation services is a desirable result of ANSP activities.

The term "aviation safety (safety)" is generally understood to mean the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level [1].

While the term "ATM security" is defined the safeguarding of the ATM system (functional system) from security threats and vulnerabilities; and the contribution of the ATM system to civil aviation security, national security and defence, and law enforcement [2].

Nowadays, the requirements for safety risk assessment are set at the state level [3-5] and include:

- risk assessment of changes in ATM system (functional system);
- assessment of existing risks in the ATM system based on the results of monitoring and analysis;
- risk assessment performed on the basis of post safety related occurrences and (or) on the results of investigation thereof.

In addition to this ANSP must establish risk assessment procedure regarding ATM security (including information security).

It should be noted that research has tended to focus on Safety risk assessment rather than ATM Security risk assessment. Without a doubt, taking into account current trends in the field of ANSP digital transformation, the problem of information and cyber security risk assessment (as a part of ATM Security) is actual and poorly research.

This article considers the field of safety and ATM security risk assessment as the main subject of its study.

By and large, ATM system infrastructure protection is described as a set:

$$ATM_{\text{sec}} = \{InfSEC, PhSEC, HrSEC\}, \quad (1)$$

where $InfSEC$ –information security – the application of security measures to protect information and data processed, stored or transmitted in ITS and communication, navigation and surveillance (CNS) equipment against loss of integrity, confidentiality and availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves; $PhSEC$ – physical security – the part of security concerned with physical measures designed to safeguard people and prevent unauthorized access to CNS equipment, facilities, material and documents [2]; $HrSEC$ – personnel security – the part of security concerned with procedures designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorized to have initial and continued access to classified information and controlled areas without constituting an unacceptable risk to security.

Analysis of the literature [6, 7] showed that there are global vision for the problem of cybersecurity in

aviation industry, however, there aren't any practical examples regarding the impact of information and cyber security threats on aviation safety.

Aviation safety risk assessment procedure is regulated by the relevant requirements and international standards. ANSP usually uses a number of techniques and methods recommended by International Civil Aviation Organization (ICAO) [1] and The European Organization for the Safety of Air Navigation (EUROCONTROL) [8] for risk assessment and mitigation.

Nevertheless, these methods haven't been adopted to assess ATM security risks. One of the most complicated task during risk assessment is to identify information security threats and hazard in ATM system. It happens due to a limitation of research and statistic data.

The work [12] shows us the research of information space and information flows of ANSP. The proposed functional model [12] is necessity for information threats identification and safety hazard assessment procedure.

The purpose of the article is the development of a functional hazard assessment model regarding information security as a part of ATM security risk management method which can be implemented by ANSP.

As a result, it provides ANSP an opportunity to increase the effectiveness of risk management to ensure information security and cyber security at the levels of the organization and information system.

Risk management is a key component of safety and ATM security management and includes aviation safety hazard identification, risk assessment, risk mitigation and risk acceptance.

The proposed model of functional hazard assessment regarding information security

The ICAO Manual [1] highlights the importance of distinguishing between hazards (the potential to cause harm) and risk (the likelihood of that harm being realized during a specified amount of risk exposure).

The risk assessment is connected with studies and identification of possible hazards associated with operation of ATM system.

The risk assessment is based on the evaluation of the criteria is described as a set:

$$SC_r = \left\{ Sev_{HAZ}, Pr_{OCC}, Tol_{ef} \right\}, \qquad (2)$$

where Sev_{HAZ} – the severity of a hazard; Pr_{OCC} – the probability (frequency) of its occurrence; Tol_{ef} – tolerability of its effects.

The aim of functional hazard assessment is the identification of: a list of hazards (*HAZ*) and causes (*CAU*); effects on the operational activities of ANSP (*Ef*); severity of potential hazards.

The first stage of functional hazard assessment for the ANSP is to identify the causes of their occurrence in the ATM system.

ATM system information infrastructure consists of elements and it is described as a set:

$$ATMinf = \left\{ ATCSys, ITS, VCS, SUR, COM \right\}, \qquad (3)$$

where $ATCSys$ – Automated Air Traffic Control Systems; ITS – Information and Telecommunication Systems; VCS – Voice Communication Systems; SUR – Surveillance Systems; COM – Communication Systems.

The block diagram of the relationship between information security risk assessment and aviation safety is presented in Fig. 1.

A comparative analysis of ICAO and EUROCONTROL severity classes names [1, 9] is given in Table 1.

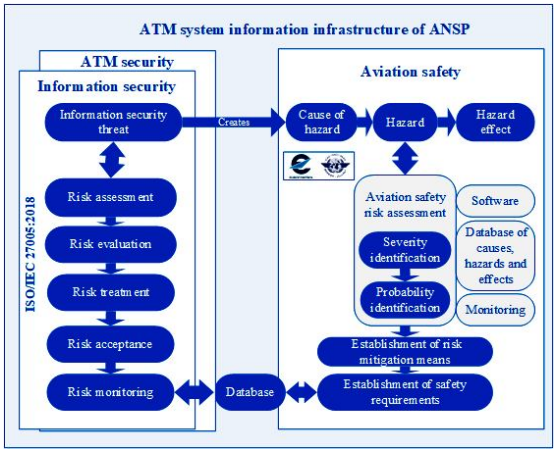

Fig. 1. Structural diagram of the relationship between information security and safety

Table 1 –**Comparative analysis of severity classes names**

Severity classes names		Number of classes
ICAO [1]	**EUROCONTROL [9]**	
Catastrophic	Accident	1
Hazardous	Serious Incident	2
Major	Major Incident	3
Minor	Significant Incident	4
Negligible	No Safety Effect	5

The list of identified typical causes of hazards, hazards and effects associated with information security threats is presented in tabl. 2 – 4.

Assessment of the severity class of the identified hazards (*HAZ*) was performed using classification schemes in ATM system [9-11]. This assessment was made by experts in a formalized view in accordance with the scheme [1, 5].

Table 2 – **The list of identified causes of hazard**

***ATMinf* elements**	**Causes of hazard**	
	ID	**Description**
ATC Sys	*Cau01*	Radar data pre-processing subsystems failure
	Cau02	Radar data processing (RDP) subsystems failure
COM	*Cau03*	Aeronautical ground telecommunication facilities failure

ATMinf elements	Causes of hazard	
	ID	Description
ATC Sys	*Cau04*	Flight data processing (FDP) servers failure
	Cau05	Failure of aeronautical fixed telecommunication network (AFTN) channels
	Cau06	Online Data Interchange (OLDI) server failure
ATC Sys	*Cau07*	Local Area Network (LAN) failure
ITS		
ATC Sys	*Cau08*	Data recording and playback server failure
	Cau09	External time reference system failure
	Cau10	Equipment failure of one of the two workplaces
	Cau11	Voice communication systems failure
VCS		
SUR	*Cau12*	Surveillance systems failure
COM	*Cau13*	Communication equipment failure
ITS	*Cau14*	AFTN equipment failure
	Cau15	Reducing the capacity of AFTN channels
ATC Sys	*Cau16*	Safety Nets (SNET) servers failure
	Cau17	Equipment failure of two workplaces

Table 3 – **The list of identified hazards**

Елемент *ATMinf*	Hazard	
	ID	Description
ATC Sys	*HAZ01*	Complete loss of surveillance systems data
ITS		
SUR		
ATC Sys	*HAZ02*	Partial loss of surveillance systems data
ITS		
SUR		
ATC Sys	*HAZ03*	Partial loss of flight data
ITS		
ATC Sys	*HAZ04*	OLDI unavailability
ITS		
ATC Sys	*HAZ05*	SNET and Monitoring Aids (MONA) unavailability
ATC Sys	*HAZ06*	Complete or partial loss of recording and playback data
ATC Sys	*HAZ07*	Complete loss of Air Traffic Control System (ATCS) data in the workplace
VCS	*HAZ08*	Complete / partial loss of "air-ground" communication for more than 5 minutes
ITS		
COM		
ATC Sys	*HAZ09*	Loss of automatic coord. functions.
ITS	*HAZ10*	Loss of automatic updating function of System Flight Plans (SFPLs) and airspace use restrictions.
ATC Sys	*HAZ11*	Unavailability information from external time reference system
ITS	*HAZ12*	Loss of automatic radar and planned data correlation
ATC Sys		
ATC Sys	*HAZ13*	Complete loss of ATCS data
ATC Sys	*HAZ14*	Loss of the function of automatic updating of flight plans, airspace use restrictions, NOTAM
ITS		

Table 4 – **The list of identified effects**

ID	Description
Ef01	Serious inability to ensure safety
Ef02	Surveillance data unavailability on ATCS workplaces
Ef03	Significant workload on air traffic controllers
Ef04	Significant reduction of air traffic service (ATS) sectors capacity
Ef05	Separation minima infringement
Ef06	Partial surveillance data unavailability on ATCS workplaces
Ef07	Significant workload on air traffic controllers in certain sectors
Ef08	Significant reduction of certain air traffic service sectors capacity
Ef09	Workload on air traffic controllers
Ef10	Restrictions on the provision of planning information required for ATS
Ef11	Unavailability to modify airspace use restrictions and availability of ATS routes
Ef12	Planning information irrelevance
Ef13	Partial loss of flight data
Ef14	Aeronautical Information Service (AIS) information unavailability
Ef15	Lack of automatic modification of airspace use restrictions and availability of ATS routes
Ef16	No warnings of SNET
Ef17	Impossibility to identify aircraft via surveillance systems
Ef18	Lack of correlated radar and planning data
Ef19	Lack of recording and playback data
Ef20	Desynchronization of external time reference system data
Ef21	Disappearance of data at the air traffic controllers workplace
Ef22	ATS sectors capacity reduction
Ef23	Significant reduction of defined air traffic service sectors capacity
Ef24	Significant separation minima infringement

Analytic hierarchy process [13-15] was applied for quality and quantity hazard functional assessment.

Table 5 and Fig. 2, 3 demonstrate the generalized results of the functional assessment of the severity classes of the identified hazards that are associated with information security threats. EUROCONTROL [8,9] and ICAO [1] safety risk classification schemes were applied.

According to the results of the analysis of identified hazards (Fig. 2) we can conclude that four hazards have a second class of severity – a serious incident, two hazards have a third class of severity – a major incident, six hazards – a fourth class (significant incident) and two hazards no safety effect.

Serious incidents are [9]:

- large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation;

- one or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).

Table 5 – **Functional hazard assessment results**

Hazard ID	Severity	Probability	Safety objective
HAZ01	Class 2 – Serious Incident / Hazardous	Improbable	Hazard can happen once in 3 years
HAZ08			
HAZ11			
HAZ12			
HAZ02	Class 3 – Major Incident / Major	Remote	Hazard can happen once in 6 months
HAZ13			
HAZ03	Class 4 - Significant Incident / Minor	Occasional	Hazard can occur once every 10 days
HAZ05			
HAZ07			
HAZ09			
HAZ10			
HAZ14			
HAZ04	Class 5 - No Safety Effect / Negligible	Frequent	
HAZ06			

The software model of functional hazard assessment regarding information security

In order to rectify the problem of automation and visualization the process of safety risks assessment regarding information security threats, a software (program model) was developed via MATLAB Fuzzy Logic Toolbox [16, 17]. ICAO method for safety risk assessment was taken as a basis [1] and this method was improved in order to take into account the impact of information security threats on the ANSP activities.

The following parameters were taken into account when assessing the safety risk (acceptability) based on the use of a fuzzy network:

A_n – measure of the causes of the hazard regarding information security threats;

SAF_P – hazard severity;

SAF_P – hazard probability;

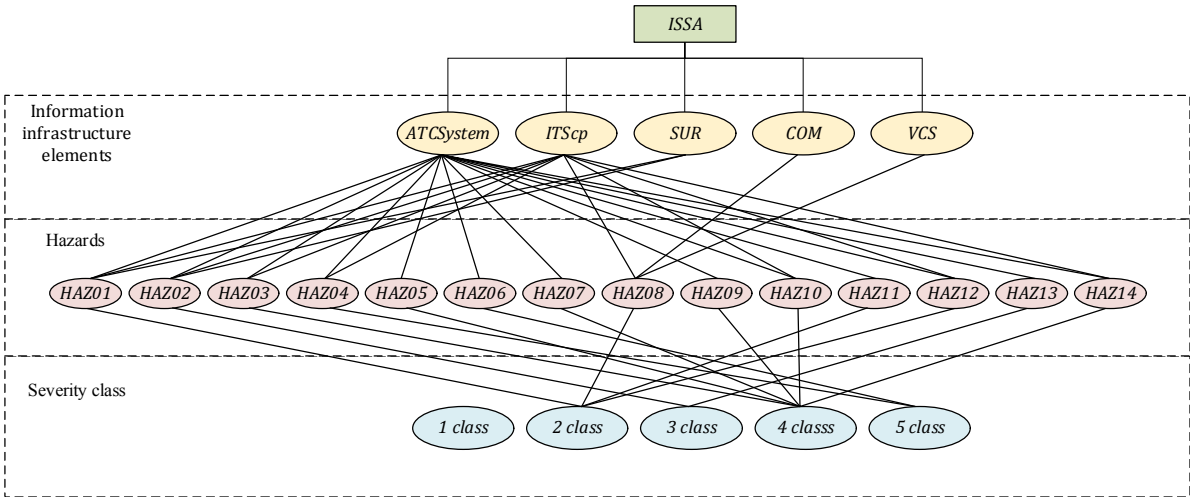

Fig. 2. Hierarchical model of qualitative functional risk assessment

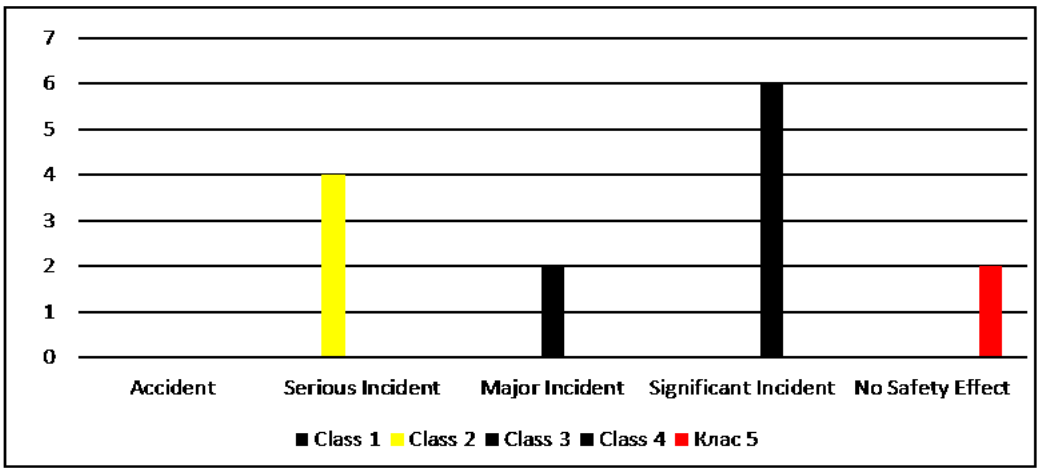

Fig. 3. Distribution of identified hazards by severity classes

Table 6 shows the qualitative and quantitative indicators of the above parameters.

A fuzzy network (Takagi-Sugeno-Kanga model) with an appropriate structure and the necessary set of parameters has been developed for the software model for safety risk assessment associated with (Fig. 4) [18-20].

Risk_tolerability – the value of safety risk, calculated as follows:

$$SAF\_R = (A_n + SAF\_P + SAF\_S)/3 \qquad (4)$$

The input data (SAF_R) is a given scale of risk acceptability, which consists of three levels according to the safety risk assessment ICAO method [1] (acceptable, tolerable, intolerable). The graphical interface of the program for viewing the rules is presented in Fig. 5.

Table 6 – **Qualitative and quantitative indicators**

Symbol	Qualitative representation	Quantitative representation
A_{pl}	Very low	$A_{pl} = 0{,}2$
	Low	$A_{pl} = 0{,}4$
	Average	$A_{pl} = 0{,}6$
	High	$A_{pl} = 0{,}8$
	Very High	$A_{pl} = 1$
SAF_S	Negligible	$SAF\_S = 0{,}2$
	Minor	$SAF\_S = 0{,}4$
	Major	$SAF\_S = 0{,}6$
	Hazardous	$SAF\_S = 0{,}8$
	Catastrophic	$SAF\_S = 1$
SAF_P	Extremely improbable	$SAF\_P = 0{,}2$
	Improbable	$SAF\_P = 0{,}4$
	Remote	$SAF\_P = 0{,}6$
	Occasional	$SAF\_P = 0{,}8$
	Frequent	$SAF\_P = 1$

The appearance of the output surfaces of the fuzzy set rules is shown in Fig. 6.

Here we solve several problems simultaneously. The above visualization can provide information security experts information regarding risk acceptability at the level of ANSP.

Quantitative safety risk assessment associated with information security threats was performed using mathematical expression (4), Fuzzy Logic software and fuzzy inference rules. Based on the assessment results, a hierarchical model for safety risks was built (Fig.7). According to ICAO scale [1] for hazards *HAZ*01 – *HAZ*14 the risk tolerability is set as tolerable. Tolerable risk can be tolerated based on the safety risk mitigation. It may require management decision (information security requirements) to accept the risk.

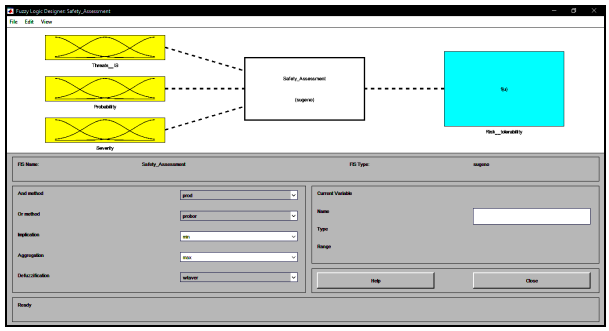

Fig. 4. The general structure of a fuzzy safety risk assessment network

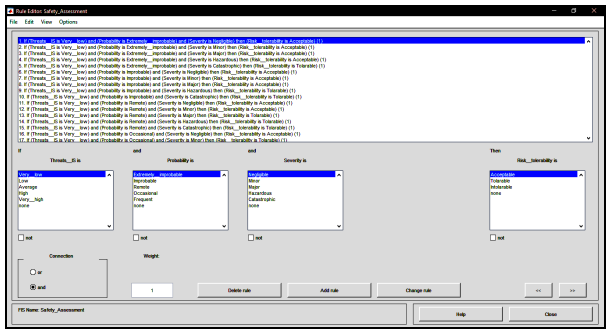

Fig. 5. Fuzzy network rule editor interface

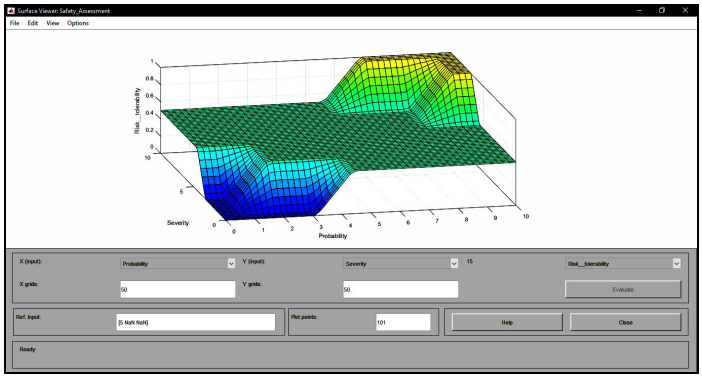

Fig. 6. Fuzzy set rule output surface viewer

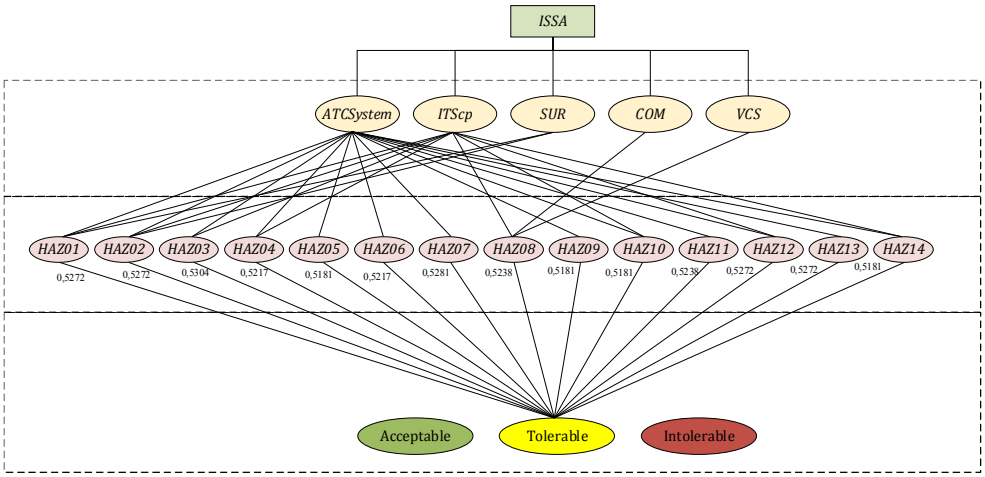

Fig. 7. Hierarchical model of safety risk assessment

The proposed set of information security requirements for air navigation service providers

Information security requirements (ISR) must be established in order to get acceptable safety risk tolerability.

A list of such ISR is offered (Table 7).

Table 7 – **The list of proposed ISR**

ID	Description
ISR01	ANSP must introduce an information security risk management process within the ANSP risk management system.
ISR02	ANSP must implement a risk-oriented approach and security measures in accordance with ISO/IEC 27001 (Annex A) and ISO / IEC 27002.
ISR03	ANSP must define all critical business processes as a minimum scope of information security management system (ISMS). ANSP has the right to expand the scope of ISMS.
ISR04	ANSP must form a security management division for ISMS implementation and operation or delegate to existing ANSP management division. ANSP must develop regulations on this management division. The regulation should include a clear tasks, functions and responsibilities for information security risk management.
ISR05	ANSP must develop and implement an information security policy (ISP). ISP should include following: 1) information security goals; 2) the scope of information security policy; 3) principles, rules and requirements of information security in the ANSP departments and divisions; 4) definition of functions (roles) and responsibilities for information security.
ISR06	ANSP must support the information security policy and review it at least once a year.
ISR07	ANSP must approve the information security policy and communicate its content to all personnel and, if necessary, to third parties.
ISR08	ANSP must develop and approve an information security development strategy.
ISR09	ANSP must develop and approve a business continuity plan and contingency plan. These plan takes into account the continuity of information security measures as part of the ANSP business continuity management process.
ISR10	ANSP must appoint a Chief Information Security Officer (CISO). CISO provides: 1) strategic management for information security at the level of ANSP; 2) determination of directions for the development of information security; 3) compliance of information security measures with the business processes of ANSP; 4) control over the implementation of information security measures in ANSP departments.
ISR11	ANSP must familiarize employees with the information security policy of the ANSP when hiring.
ISR12	ANSP must familiarize employees with internal documents establishing information security requirements.
ISR13	ANSP must implement information security awareness / training program for employees
ISR14	ANSP must introduce measures to control access to information infrastructure facilities.
ISR15	ANSP must develop and implement a policy for the use of cryptographic tools to protect information.
ISR16	ANSP must define a standard reference time source and ensure that operating systems are synchronized with it.
ISR17	ANSP must develop and implement information security measures regarding wireless data transmission networks.
ISR18	ANSP must ensure the placement of servers and equipment providing the ANSP services in the demilitarized zone of ANSP information infrastructure.
ISR19	ANSP must develop and approve internal documents that establish requirements for information security, maintenance, operation of CNS equipment
ISR20	ANSP must develop and approve a document on the use of email.

Taking into account the implemented ISR, the functional hazard assessment is shown in Fig. 8.

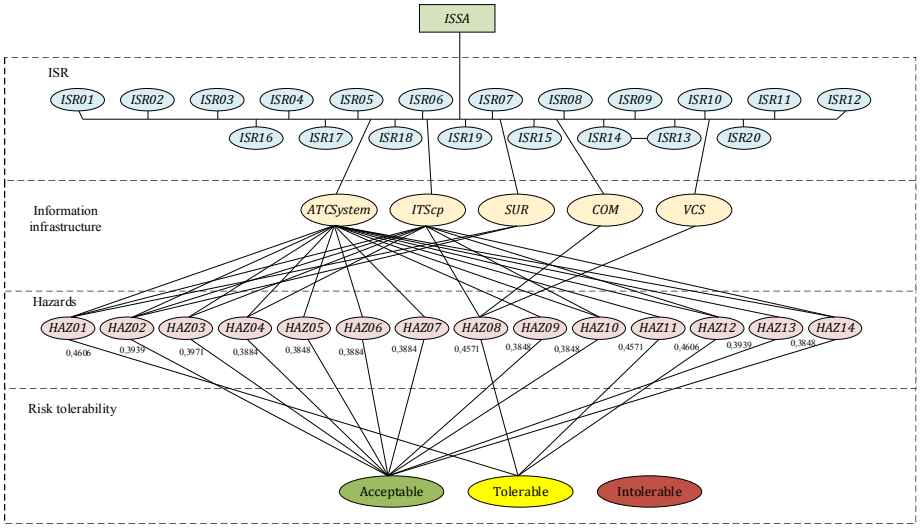

Fig. 8. Hierarchical model of safety risk assessment with implemented ISR

These techniques have potential to solve contemporary problems in safety risk assessment regarding information security. Considering the results obtained from studies evaluating fourteen hazards, it can be concluded that the risk tolerability for ten hazards has become acceptable.

Overall, our results demonstrate a strong effect of ISR. Nevertheless, for *HAZ*01, *HAZ*08, *HAZ*11, *HAZ*12 risk tolerability is still tolerable. This aspect of the research suggested that ANSP must monitor these hazards and causes.

Conclusions

The article indicates that the problem of risk assessment regarding information security is actual at the level of ANSP. As far as we know, no previous research has investigated the influence information security threats on safety. This remains an open problem in this area.

The number of typical safety hazards is possible to identify using the proposed model of functional hazard assessment.

It becomes possible to establish severity classes according to the EUROCONTROL and ICAO scales for all identified hazards.

A qualitative and quantitative hazard assessment, risk tolerability, information security requirements has been carried out.

On this basis, we conclude that the most critical identified hazards for safety are:

*HAZ*01 – complete loss of surveillance systems data;

*HAZ*08 – complete / partial loss of "air-ground" communication for more than 5 minutes;

*HAZ*11 – unavailability information from external time reference system;

*HAZ*12 – loss of automatic radar and planned data correlation.

The software model for safety risk assessment has been developed on MATLAB Fuzzy Logic Toolbox. The model allows obtaining values (quantitative and qualitative) on the acceptability of safety risks in the event of information security threats.

A set of rules for fuzzy inference was formulated and it covers all possible combinations of input variables and contains 125 rules for safety risk assessment.

Additionally, this model is appropriate for safety risk assessment regarding changes in ATM system of ANSP.

The implementation of these risk assessment models allows ANSP to make organizational and technical decisions. Furthermore, the implementation will allow ANSP to:

- increase the level of information security maturity of ANSP operating divisions;
- increase the level of maturity of ATM security system;
- identify of information infrastructure elements vulnerabilities;
- identify of potential safety hazards, their causes and effects;
- organize and protect of ANSP information infrastructure from various types of information and cyber security threats;
- reduce the likelihood of information and cyber threats, conditions or circumstances that can cause an aircraft accident or incident;
- eliminate of incidents and unacceptable risks.

Regardless, future research could continue to develop web-application (online toolkit) for information risk assessment of ANSP.

References

1. *ICAO Safety Management Manual* (2018), Doc.9859 Fourth Edition.
2. *ICAO Air Traffic Management Security Manual* (2013), Doc.9985 First edition.
3. *Air Code of Ukraine* (2011), 19.05.2011 No. 3393-VI.
4. *Rules for Certification of Entities Providing Air Navigation Services* (2007), Order of the Ministry of Transport and Communication of Ukraine No. 42 dated 22.01.2007 (registered, Ministry of Justice of Ukraine on 07.02.2007 No. 104/13371).
5. *Regulation for Safety Oversight in Air Traffic Management System* (2010), approved by the Order of Ministry of Transport and Communications of Ukraine No. 320 dated on 31.05.2010 (registered, Ministry of Justice of Ukraine on 30.06.2010 No. 446/17741).
6. *ICAO Aviation Cybersecurity Strategy* (2019), available at: https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.
7. *CANSO Standard of Excellence in Cybersecurity* (2020), available at: https://canso.fra1.digitaloceanspaces. com/uploads/2020/09/CANSO-Standard-of-Excellence-in-Cybersecurity.pdf.
8. *EUROCONTROL; Safety Assessment Methodology* (2006), Version 2.1, November 2006.
9. *ESARR4: Risk Assessment and Mitigation in ATM* (2001), available at: https://www.eurocontrol.int/sites/default/files/2019-06/esarr4-e10.pdf.
10. *Acceptable means of compliance with ESARR 4* (2009), available at: https://www.eurocontrol.int/sites/default/files/2019-06/eam4-amc-e4.0.pdf.
11. *ED 125*, Process for Specifying Risk Classification Scheme and Deriving Safety Objectives in ATM "in compliance" with ESARR 4.
12. Chernysh V. I. (2020) "Research of information space and information flows of air navigation service providers", *Telecommunication and information technology,* vol. 2 (2020), pp. 51 – 59.
13. Chernysh V.I., Zamula A.A. (2012) "Analytic hierarchy process for information risks assessment", *Scientific and technical conference with international participation "Computer modeling in high technology (KMNT-2012)". Conference materials*, pp. 145-149.

14. Chernysh V.I. (2012) “Methodology for assessing information risks using Analytic hierarchy process” *Radio electronic and computer systems,* Vol.1 (53), pp. 46 – 50.
15. Saaty, Thomas, Alexander, Joyce (1989), *Conflict Resolution: The Analytic Hierarchy Process*. New York, New York: Praeger.
16. Shtobva S. D. (2007), *Design of fuzzy systems using MATLAB*, Hot line – Telecom, 288 p.
17. Leonenkov A.V. (2005), *Fuzzy modeling in MATLAB and fuzzyTECH*, BHV-Petersburg, 736 p.
18. Jin Y., Seelen W., Sendhoff B. (1999), “On generating flexible, complete, consistent and compact (FC3) fuzzy rules from data using evolution strategies”, *IEEE Transactions on Systems, Man, and Cybernetics*, No. 29 (4). pp. 829-845.
19. Sommestad T., Ekstedt M., Johnson P.A. (2010), “Probabilistic relational model for security risk analysis”, *Computer & Security*, Vol. 29, No. 6. pp. 659-679.
20. Sug B., Han I. (2003), “The IS risk analysis based on business model”, *Information and Management*, Vol. 41, No. 2. pp. 149-158.

Надійшла (received) 28.07.2020
Прийнята до друку (accepted for publication) 07.10.2020

ВІДОМОСТІ ПРО АВТОРА / ABOUT THE AUTHOR

Черниш Владислав Ігорович– голова правління громадської організації «Цивільна авіація України», Київ, Україна;
Vladyslav Chernysh– Chairman of the Board, Non-governmental organization “Civil Aviation of Ukraine”, Kyiv, Ukraine;
e-mail: v.chernysh@aviation.org.ua; ORCID ID: https://orcid.org/0000-0002-0443-1946.

Модель функціональної оцінки небезпек в системі організації повітряного руху щодо реалізації загроз інформаційної безпеки

В. І. Черниш

Анотація. Загроза інформаційній безпеці для постачальників послуг з аеронавігаційного обслуговування представляє потенційне порушення інформаційної безпеки елементів інформаційної інфраструктури в системі організації повітряного руху, таких як обладнання зв'язку, навігації та спостереження, а також інформаційно-телекомунікаційних систем. Як правило, загроза виникає внаслідок присутності вразливих компонентів у захисті інформаційних технологій як частини діяльності постачальників послуг з аеронавігаційного обслуговування. Більшість підходів та методів міжнародних авіаційних організацій та найкращих практик постачальників послуг з аеронавігаційного обслуговування зосереджені на розробці методів та моделей ризику щодо безпеки польотів. Загальновідома проблема оцінки ризиків безпеки польотів полягає в тому, що вона не враховує загрози інформаційної та кібер безпеки. **Предметом** статті є дослідження методів та моделей для оцінки ризиків постачальників послуг з аеронавігаційного обслуговування. **Метою** є розробка моделі функціональної оцінки небезпек та набору вимог інформаційної безпеки для постачальників послуг з аеронавігаційного обслуговування. Запропонована модель функціональної оцінки небезпек відрізняється від відомої деталізацією напряму інформаційної безпеки. Програмна модель функціональної оцінки небезпек була розроблена за допомогою MATLAB Fuzzy Logic Toolbox. **Практичне значення** полягає в тому, що отримані результати дозволяють постачальникам послуг з аеронавігаційного обслуговування приймати кращі рішення щодо вдосконалення зрілості систем управління.

Ключові слова: провайдер надання послуг з аеронавігаційного обслуговування; обслуговування повітряного руху; ризик; безпека; організація повітряного руху; інформаційна безпека; загрози.

Модель функциональной оценки опасностей в системе организации воздушного движения относительно реализации угроз информационной безопасности

В. И. Черныш

Аннотация. Угроза информационной безопасности для поставщиков аэронавигационного обслуживания представляет собой потенциальное нарушение информационной безопасности элементов информационной инфраструктуры в системе организации воздушного движения, таких как оборудование связи, навигации и наблюдения, а также информационные и телекоммуникационные системы. Обычно угроза возникает из-за наличия уязвимых компонентов защиты информационных технологий в рамках деятельности поставщиков аэронавигационного обслуживания. Большинство подходов и методов международной авиационных организаций и передовой практики поставщиков аэронавигационного обслуживания сосредоточены на разработке методов и моделей риска в отношении безопасности полетов. Известная проблема оценки рисков для безопасности полетов заключается в том, что она не принимает во внимание угрозы информационной и кибер безопасности. **Предмет** статьи – исследование методов и моделей оценки рисков поставщиков аэронавигационного обслуживания. **Целью** является разработка модели функциональной оценки опасностей и набора требований к информационной безопасности для поставщиков аэронавигационного обслуживания. Предлагаемая модель функциональной оценки опасностей отличается от известных детализацией направления информационной безопасности. Программная модель функциональной оценки опасностей была разработана с помощью MATLAB Fuzzy Logic Toolbox. **Практическое значение** заключается в том, что полученные результаты позволяют поставщикам аэронавигационного обслуживания принимать более обоснованные решения относительно повышения зрелости систем управления.

Ключевые слова: провайдер предоставления услуг по аэронавигационному обслуживанию; обслуживание воздушного движения; риск; безопасность; организация воздушного движения; информационная безопасность; угрозы.