ASPECTS OF CYBER-SECURITY IN CIVIL AVIATION

V. Shapkin, D. Demin, A. Nikitin and A. Pleshakov
The State Scientific Research Institute of Civil Aviation,
Mikhalkovskaya Street, 67, building 1, 125438 Moscow, Russia

S. Musin
Tekhnodinamika joint-stock company,
Bol'shaya Tatarskaya Street, 35, building 5, 115184 Moscow, Russia

V. Solomentsev
Azimut joint-stock company,
Naryshkinskaya Avenue, house 5, structure 2, 125167 Moscow, Russia

ABSTRACT

The paper deals with a complex of problems of civil aviation, which arose in connection with the updating of the legal framework in terms of the implementation of the Doctrine of information security of civil aviation and the adoption of the Federal law №187 “On the security of critical information infrastructure of the Russian Federation”. The authors propose a unified approach to determining the sequence of actions needed for the development of effective appropriate protective measures aimed at preventing cyber-attacks in civil aviation. Principles are formulated that enable systematic work at the national level to ensure aviation cyber-security. The problems of national regulation are discussed that relate to cyber-security issues and determination of the cyber-security place as an element of the complex comprising transport security, aviation security and flight safety.

Keywords: International Civil Aviation Organization, critical information infrastructure, transport security, flight safety, aviation cyber-security, cyber threat, process approach, cyber-security.


http://www.iaeme.com/IJCIET/issues.asp?JType=IJCIET&VType=9&IType=10
1. INTRODUCTION

To date, when it would seem that modern technologies are aimed at maintaining the effective operation of almost any field of human activity, a very serious question arises as to how safe the use of air transport is. It is quite fair to say that over the past years specialists have achieved high resiliency of airborne equipment and ground control systems, but, according to most experts, cyber-security is not given due consideration, and this is due to a number of reasons: from the lack of a proper legal and regulatory framework that takes the specificity of the industry into account, to the high international integration of information and communication systems of civil aviation.

Over the past few years, issues of cyber-security in civil aviation have been receiving increasing attention from both the International Civil Aviation Organization (ICAO) and national authorities that regulate the industrial activities.

In May 2016, ICAO, within the framework of the 39th Assembly, issued working paper A39-WP/17, “Addressing Cyber-security in Civil Aviation,” [1] with the request for governments and industry stakeholders to take action to counter cyber-threats in civil aviation.

In May 2018, ICAO’s Secretary General, Dr. Fang Liu, addressed government and industry experts in Bucharest, participating in the opening of the Europe, Middle East and Africa (EMEA) Cyber-security in Civil Aviation Summit. Dr. Liu pointed out that in such a complex industry as air transport, one cannot overlook the fact that even one cyber-security-related incident may affect the work of many companies and stakeholders; there are new and more sophisticated online digital processes that are launched almost daily and affect the effectiveness of the network management and the ability of airlines and airport operators to serve their customers [2].

According to the assessments performed by the insurance sector, combined threats, including cyber-crime, IT failures and database crackings were the third most significant risk to global business in 2017; Dr. Liu noted that ICAO is currently working hard to formulate policies and strategies to ensure cybersecurity in civil aviation, and that the new Global Aviation Security Plan will make a significant contribution to global coordination and information sharing, which are key to successful anti-threat measures [2].

At present, the Russian Federation has adopted a number of regulatory acts aimed at providing various aspects of national information security for the sustainable functioning of the critical information infrastructure of the Russian Federation with respect to computer attacks against the country. These apply to state authorities, state institutions, Russian legal entities and (or) individual entrepreneurs who own, lease or otherwise legally own information systems, information and telecommunications networks, automated management systems that operate in the field of health, science, transport, communications, energy, banking and other areas of the financial market, fuel and energy complex, in the field of atomic energy, defense, rocket and space, mining, metallurgical and chemical industries, Russian legal entities and (or) individual entrepreneurs ensuring the interaction of these systems or networks.

These regulatory acts have been developed for several years, and in this process general formulations were followed without taking into account the industry-specific issues. At the request of representatives of various industries, the specifics of ensuring cyber security of the critical information infrastructure was left to the industry regulators, since it was considered that it is industry regulators, none better, that know the specifics and needs for cyber-security of each specific industry.
Thus, the existing legal and regulatory framework does not adequately cover the issues arising in the framework of ensuring the cyber-security of civil aviation as an element of the global information space, therefore, the cyber-security of civil aviation should be considered separately because of the specifics and unique features of this field.

2. KEY ASPECTS OF CYBER-SECURITY IN CIVIL AVIATION

The civil aviation system consists of a set of interconnected components, systems and networks. For many years, the potential of cyber-attacks has been increasing, which can jeopardize communication and information exchange between various aviation stakeholders, affect flight safety and aviation security, and disrupt the continuity of aviation activities [3].

The aviation industry has unique characteristics and requires a special approach to ensuring cyber-security of its facilities. On the one hand, the safety of civil aviation functioning is regulated both within the framework of ensuring transport and aviation security, and within the framework of flight safety, which creates a sufficiently deep and well-developed system of standards and rules. On the other hand, despite the fact that such a system reduces some risks of cyber-attacks over the industry, the uniqueness of the aviation industry creates problem points and barriers for effective counteraction to cyber-threats. In this regard, traditional methods of providing cyber-protection in this case work extremely inefficiently.

Such basic features may include the following:

2.1. The unique infrastructural complexity of civil aviation

New trends such as the progressive introduction of remotely piloted aircraft systems and the continuous evolution of the ATM system (e.g. SWIM), airport infrastructure, service structures and the use of equipment and systems of transnational suppliers and developers strengthen the interconnection and integration of IT systems in the industry (see the Figure below), which leads to an increase in the risks of successful cyber-attacks.

![Infrastructural complexity of civil aviation](http://www.iaeme.com/IJCIET/index.asp)

The facilities of the civil aviation infrastructure are extremely diverse: from information systems on board aircraft to loyalty systems of airlines. Airports and air traffic management services are presented as extremely complex, large-scale, critically important and potentially dangerous facilities that undoubtedly attract the attention of a huge number of cyber-criminals. Accordingly, complex support for the operation of such large-scale facilities requires the presence of extremely complex and interconnected information components in the industry, which leads to a number of consequences and serious problems:

First, every civil aviation infrastructure entity has its own specific and unique features in terms of the development and the current state of its IT infrastructure, so even with
specialized “out-of-the-box” standard solutions for civil aviation facilities declared by suppliers and developers, it is extremely rare when universal standard means suffice without the need to refine and adapt the supplied systems and solutions when integrating them into existing business processes of these entities. Accordingly, in each such case, a unique set of vulnerabilities and cyber-security breaches is generated for civil aviation entities that can lead to disruption in the functioning of more general processes of the entire industry. Therefore, when developing proper protective measures to prevent cyber-attacks for each specific civil aviation facility, it is necessary to analyze threats to information security regarding automated control systems and critical IT systems of significant facilities of the critical information infrastructure of civil aviation and to identify their vulnerabilities; this analysis should include, but not be limited to the following set of actions:

- identification of sources of threats to information security and assessment of the capabilities (potential) of external and internal violators;
- analysis of possible vulnerabilities of a significant facility and its software and hardware;
- identification of possible methods (scenarios) for materializing (occurrence) of threats to information security;
- assessment of possible consequences from materializing (occurrence) of threats to information security;
- development of recommendations for adjustment of the architecture of a significant facility and organizational and administrative documents for the security of significant facilities aimed to block (neutralize) individual threats to information security;
- development (updating) of the basic model of threats to information security for the facility of the critical information infrastructure of civil aviation;
- Development of particular models of threats to information security for automated control systems of significant facilities of the critical information infrastructure of civil aviation.

Secondly, there is a big issue of “trust” to developers of most highly specialized IT systems and components of the APCS, most of which are proprietary, do not have open source codes and are essentially a black box for the entity. Civil aviation entities do not fully have the ability to conduct a thorough inspection of controllers, remote terminals, routers, specialized software, software complexes for automated process control or providing the operation of corporate networks, etc. for hidden functionality, malicious software or bugs [4]. This is a serious issue, since, as already mentioned above, almost any member of the aviation industry is currently unable to fully import all the IT components they need and must depend on developers of highly specialized software or hardware, some of which are transnational companies. Not to mention the fact that the bulk of the air fleet of Russian airlines is represented by foreign aircraft.

Thirdly, the complexity of the internal well-connected and highly integrated IT infrastructure of civil aviation and air traffic management, poorly controlled technical and pre-flight maintenance of air transport in “foreign” airports (there is a risk of malware penetration through unprotected service interfaces) and the intensity and volume of data flows in the industry require an integrated and comprehensive approach to cyber-security, both at national and international levels.
When ensuring the cyber-security of civil aviation at the national level, it is proposed to move to an integrated system approach and within the civil aviation infrastructure entities to consider issues of ensuring cyber-security in terms of the process approach, which falls into the general concept with the requirements of the relevant regulations and does not contradict them:

- comprehensive provision of cyber-security at all stages of the system’s life cycle, from the definition of requirements to ensure cyber-security, the development and implementation of organizational and technical protection measures, the operation of systems and to provision of security during de-commissioning;
- monitoring the state of security: the establishment of regulations for the inventory and audit of the IT infrastructure security in the industry, the procedure for detecting the signs of cyber-attacks and the reaction rules, organization of network traffic monitoring in a mode close to real time for all loops of the IT infrastructure of civil aviation, [4];
- Introduction of new requirements for suppliers of critical components for the aviation industry. For example, make the supplier disclose the source code of the software of logical controllers or IT systems to the entity of civil aviation after signing the supply contract, as well as excluding the chance of remote intervention of the manufacturer or developer in the operation of the supplied equipment or system using hidden information transmission channels;
- development of sectoral international and national methodological documents for ensuring cyber-security in civil aviation;
- Planning and development of measures to enhance the security systems of the industry’s facilities, as well as personnel training programs.

2.2. Uncertainty of the place and roles of cyber-security in civil aviation in transport security, aviation security and flight safety

The field of civil aviation cyber-security is at the intersection of aviation security, transport security, flight safety, information security and safety of automated control systems.

Aviation security is a unique component of the industry security. According to the definition of ICAO and the Air Code of the Russian Federation, aviation security is a state of aviation’s protection against illegal interference in aviation activities. It is ensured by aviation security services at airfields or airports, units of departmental security services of federal executive authorities in the field of transport, aviation security services of operators (aviation enterprises), and approved bodies authorized by federal laws.

To date, the opinions of experts are divided: some believe that cyber-security of civil aviation is part of the aviation security paradigm, while others believe that cyber-security of civil aviation should be singled out as a separate field. In the published recommended ICAO documents and national regulations, cyber-security is mentioned both in the framework of aviation security, transport security and flight safety, and in separate documents. Therefore, it can be said that there is no integration of civil aviation cyber-security and aviation security or flight safety for today, but there is also no cyber-security as a separate filed – and this situation, regarding issues of civil aviation cyber-security and the incompleteness of determining its place and role in the industry, presents serious challenges in light of the following:

- lack of clearly split functions and allocation of resources between civil aviation entities and the regulatory authorities responsible for information security, cyber-
security, and units and/or organizations responsible for aviation security, transport security or flight safety;

- lack of sectoral regulations, methodological or advisory documents in the field of ensuring civil aviation cyber-security;
- absence of a single situational and analytical center for cyber-security in the field of civil aviation that could provide scientific and methodological support in the creation of systems for ensuring cyber-security, the development of tactical and operational activities, the provision of assistance in making timely corrective management decisions in the implementation of works to ensure cyber-security and assistance in response to the onset of events and consequences associated with cyber-attacks;
- lack of a single process operation for identification of cyber-threats, risk assessment, their analysis and timely identification of cyber-security problems in civil aviation, parrying threats and rules of reaction in the case of cyber-attacks;
- Existence of mutually contradictory requirements, standards and procedures to ensure cyber-security on the one hand, and aviation security, transport security and flight safety on the other hand. The lack of harmonized requirements for cyber-security makes it difficult for the entities to act in this area and can actually double their responsibility for the same functions;
- a large number of various types of civil aviation entities, which leads to the difficulties in defining rules for calculating the values of the cyber-security criteria so that the whole industry is in a “unified system of coordinates” and it does not lead to the situation when uniform organizations with uniform critical processes and critical facilities use their own methods for criteria calculation and obtain fundamentally different conclusions about the cyber-security of similar civil aviation infrastructure facilities;
- presence of a huge number of diverse facilities, highly specialized information systems, software and hardware;
- poor training and low level of competence, lack of the necessary number of specialists working in the field of ensuring cyber-security in civil aviation;
- Terminological and conceptual discrepancies between industry representatives responsible for cyber-security and for aviation security (which may make it difficult to work together on cancellation (neutralization) of calls and responses to incidents).

3. PROBLEMS OF NATIONAL REGULATION OF THE CYBER-SECURITY ISSUES IN CIVIL AVIATION IN THE RUSSIAN FEDERATION

At the international and national level, the agenda for ensuring cyber-security in civil aviation and countering current cyber-threats is developing in a regulatory vacuum and the absence of mechanisms for joint incident management and investigation. On the one hand, the adopted regulatory acts partially regulate the collection and exchange of information on cyber-threats and the procedure for responding to them. However, they do not take into account the specific features of the industry and apply only to the critical information infrastructure entities, do not cover the whole infrastructure of the industry as a whole, since cyber-threats are often of a cross-border nature.
The complexity of regulating the issues of cyber-security lies in the unclear distribution of regulatory tasks between state authorities and departments and their large number; today there is no clear understanding of which of the structures is responsible for the development of the cyber-security strategy concept for civil aviation. This “fragmentation” leads to the absence of comprehensive work on strategic planning for measures to ensure cyber-security of the industry, difficulties in communication between organizations and the lack of a well-functioning mechanism for resolving issues that fall within the competence of several organizations at once. Also, this situation leads to the fact that it is extremely difficult to provide the necessary flexibility and efficiency of approaches to ensuring cyber-security due to the absence of a single common vector for the development of the cyber-security policy in civil aviation in the country. Given these nuances, the only organization in the Russian Federation that has all the necessary competencies, rich experience in solving complex industry problems, and can offer scientifically grounded technical, regulatory and other solutions in civil aviation as a whole should be FSUE State Research Institute of Civil Aviation, which has performed significant scientific works in ensuring security of aviation activities [5-13].

4. CONCLUSIONS

Thus, in general, the legal provision of civil aviation cyber-security in the Russian Federation is currently poorly developed, and the implementation of the adopted regulatory acts in civil aviation should be the beginning of major complex efforts aimed at the formation of a strong regulatory framework for cyber-security in the industry that would take the high international integration and a wide variety of entities of civil aviation into account.

It is necessary to prepare a concept of some cyber-security strategy for civil aviation in the Russian Federation, where, in accordance with the adopted regulatory acts, the responsibility is separated between the state and the entities of the industry. The state responsibility should include issues of timely and relevant statutory regulation of cyber-security harmonized with international practices and experience; the responsibility of entities of the civil aviation infrastructure is to ensure cyber-security of its facilities in their legitimate use, implementation and compliance with adopted standards of cyber-security; the responsibility of scientific and research organizations should be comprehensive scientific and methodological support and assistance both to the state in the preparation of regulatory legal documents, and to production entities in the implementation and compliance of the approved standards and rules for ensuring cyber-security of civil aviation.

REFERENCES


Aspects of Cyber-Security in Civil Aviation


