UDC 739.733.017.7.973.7.023.7

A.P. Sapsai, associate professor of NAU
V.V. Minitskyi
(National Aviation University, Ukraine)

Cybersecurity of civil aviation

The problem of cybersecurity problem is global in nature and a rather acute issue in today's information environment. World leaders pay more attention to cybersecurity of their own infrastructure.In the field of civil aviation security, the level of criticality is significantly increased by the increased level of communication,namely, the interaction between aircraft and ground vessels.

Modern implementation of cybersecurity technologies.

The introduction of modern technologies in sphere of communication and information on the one hand increases the level of effectiveness of civil aviation activity and the other – forms a number of new impressions and potentially dangerous threats.

Building effective cybersecurity as an integral organizational part helps organizations to increase their effectiveness by early detection of potential cyber threats. Cyber defense is critical. Today, on average, 78% of cyber-attacks worldwide are successful.

Cybersecurity in civil aviation is based on experience and successful development in the areas of advanced aviation security, as well as flight safety with which there are many common core elements. This type of cybersecurity enhances both cybersecurity and has a positive impact by promoting and strengthening aviation safety, security and cybersecurity.

In response to the need and importance of protecting important civil aviation infrastructure, information and communication systems from cyber threats, the International Civil Aviation Organization is developing a secure and reliable cybersecurity framework. Regulation A39-19 "Tackling Cybersecurity in Civil Aviation" explains the actions that need to be taken by states and stakeholders in countering cyber attacks by civil aviation on the basis of a comprehensive, inclusive collaborative approach.

In addition, the 39th Assembly of ICAO took the lead in developing a workplan and organized the Secretariat Cybersecurity Research Group (SSGC). The work of SSGC is prepare a strategic cybersecurity project and develop important mechanisms for sharing and sharing relevant and original cybersecurity information.

The 40th Session of the ICAO Assembly adopted resolution A40-10 "Solving problems of cyber security in civil aviation".

The International Air Transport Association (IATA) also works closely with ICOA on aviation cybersecurity. This organization has a positive impact on how the sphere itself responds to cybersecurity challenges. IATA is working on a cybersecurity strategy, where organization developed act called Aviation Cyber Security document.

IATA strongly supports the work of ICAO as the most appropriate organization for a coherent global dialogue and action on civil aviation on civil aviation cybersecurity. Without clear international leadership in the field of aviation cybersecurity, there is a risk of diving global standards, a complex regulatory regime that constrains growth, innovation and ability to assess risks to aviation civil cybersecurity, managing them within and outside countries.

IATA is actively involved in building the competence of stakeholders on global aviation cybersecurity requirements. IATA has designed the Aircraft Cyber Security Implementation Team (ACSTF), which works to promote dialogue and disseminate current experiences among aviation stakeholders. The development of the ACSTF has created an area of high trust where ideas for sharing specific information on a variety of related topics are considered. IATA also held a meeting with stakeholders on aviation cybersecurity in Singapore (April 2019). During this session, stakeholders explored current challenges in the aviation industry and discussed what a cyber-safe future should look like. The conclusion stresses that much has been done, but that much remains to be done.

At the same time, the issue of cyber security in the aviation industry of Ukraine regulated by the following normative-legal documents: ICAO resolution A39-19 "Solving Cybersecurity problems in civil aviation" (06.10.2016), Law of Ukraine "On the State Program of Aviation Security of Civil Aviation" (21.03.2017), Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" (05.10.2017), requiring institutions and organizations to take measures to protect against prohibited access and to protect personal and confidential information of clients and to assume responsibility for non-compliance with these requirements.

A large number of aircraft with outdated technologies and unencrypted data transfer protocols create major problems and complicate the cyber security process. European Cockpit Association (ECA) has determined that aircraft and other critical objects are vulnerable to cyber attacks and at greater risk of dangerous situations.

The EU Commission has already proposed a new process of drafting rules.

ECA has a particular advantage in the European Strategic Coordination Platform EASA (ESCP) and the European Aviation Security Plan (EPAS). Defining an information security management system according to the same principle as SMS for aviation security with mandatory messages about aviation cyber events is a bright example.

ECA encourages the development and growth of European Cybersecurity Center in Aviation (ECCSA) and supports such areas at the international level (ICAO).

ECA believes cyber threats are significant and growing threat to aviation security. Thus, ECA is firmly convinced that this issue should be resolved on time.

Conformity check should be carried out by the authorities. ECA believes that this topic is best solved by requiring the National Civil Aviation Security Program (NCASPs) to contain a mandatory section on cyber security, which should deal with issues comprehensively and qualitatively.

The European Commission should define the requirements to be met to cover issues of management, risk assessment and testing.

According to the ECA, the aviation system lacks information exchange, so cyber risks are not always clear to the states and relevant stakeholders. IF the parties shared information about security breaches, attacks and experiences, global security would be more productive.

Having analyzed, cybersecurity in civil aviation is vital to security. All stakeholders, both public and private, should be involved and engaged in this area. Civil aviation cybersecurity should also involve academics.

At this stage, cybersecurity in civil aviation is beginning to develop actively, many companies are connecting to this issue. But the most important drawback in the opinion of the ECA at the current stage of cybersecurity development in civil aviation is the lack of effective information exchange between companies and countries, which increases the chances of cyber threats, which are actually incomprehensible to countries and organizations. In oder to avoid these cyber threats, private companies and states must cooperative with each other and share experiences.

References

1. Kharchenko V.P. Cyberterrorism in aviation transport/ V.P. Kharchenko, O.G. Korchenko, Yu. B. Chebotenko, E.V. Patsira, S.O. Gnatjuk // Problems of informatization and management: Zb. Science. etc: W. 4 (28). – B.: NAU, 2009. – P. 131-140.
2. Lahno V. Cybersecurity of information and communication systems of transport / V. Lahno // Security of information. – 2016. – T. 22, № 1. – P. 44-50.
3. Assembly Resolutions in Force (as of 4 Otober 2019). ICAO. 2019. URL: https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf.