UDC 347.121.2 (477)(043.2)

CERTAIN ASPECTS OF INFORMATION PROTECTION IN THE FIELD OF COMPUTER SECURITY OF AVIATION

Oleg Adamenko
National Aviation University, Kyiv

Scientific adviser – Sofia Lykhova, Doctor of Law, Professor

Keywords: information security, cyber threat, information protection, civil aviation, compliance.

Currently, the National Aviation University is a pioneer in teaching the course "Prevention of criminal offenses in the field of computer safety of aviation", designed, first of all, for the second master's level of higher education in the specialty 262 "Law Enforcement".

Currently, the vast majority of business entities in the aviation industry face many challenges in the field of data security. First of all, it is necessary to ensure the security of personal data, because the airline can process tens of millions of passenger records during the day. Aircraft, crews and passengers on board must also be under cyber defence.

In times of digitalization, when most flight tickets are purchased via the Internet, the airline processes a large amount of highly sensitive information such as bank card details, passport numbers, telephones, customer names and surnames, etc. A leak of such data or a cyberattack can have serious consequences. Therefore, at the present stage, the issue of ensuring the cybersecurity of civil aviation has ceased to be the subject of attention only for IT specialists.

This is due to the fact that the data operated by the airline is somehow connected with the personal data of either customers or employees and other individuals who provide services to the company. After the introduction of the requirements of the new EU Regulation 2016/679 on the protection of individuals regarding the processing of personal data and the free movement of such data dated 27.04.2016,

many airlines have a need to introduce the position of Data Protection Officer (DPO), the main purpose of which was to ensure the performance of functions for regulatory and organizational support of business processes related to the processing and protection of personal data.

Personal data protection officers in modern conditions should understand both the technical component of cybersecurity issues and have knowledge of regulatory support for cybersecurity and personal data protection. In practical terms, their work is connected both with a thorough study of national, European and international regulations and standards in the field of personal data protection and cybersecurity, as well as with the development of internal company documents on these issues, as well as control over their implementation.

First of all, it is worth paying attention to certain technical aspects of cybersecurity in the field of civil aviation, necessary for the formulation of further regulatory recommendations.

According to A. Ilyenko, Ukraine for the first time suffered a cybernetic attack on computer systems and the central server of Boryspil and Kharkiv airports in June 2017, which led to failures in aircraft maintenance and delayed departures. A few months later in October 2017 – the delay in the departures of aircraft from the Odessa airport as a result of hacking the computer network of the airport, which led to the loss of confidentiality of information. According to experts from the European Aviation Safety Agency (EASA), during 2019, the world's aviation systems were subjected to monthly cyberattacks up to 1000 times. Thus, approaches to countering cyber attacks should be systemic, reliable and comprehensive, the aviation industry belongs to the objects of critical transport infrastructure of Ukraine. The safety program for the transmission of critical information in the relevant aircraft avionics systems must be designed to protect, reliable, integrity and security the network and data. Effective security of transmission of critical information in computer-integrated aviation systems is aimed at combating various threats and prevents them from entering or spreading in aircraft avionics systems.

The most common threats include: viruses, Trojan horses; hacker attacks; provoking pseudo-failures during the operation of various FS

and aircraft complexes when in fact the systems are in working condition; interception and theft of data; the activities and influence of hostile intelligence agencies, etc. A successful attack can lead to complications in the operation of the functional systems of the aircraft of the development of complications of flight conditions, and in case of an increase in false data on flight conditions – to emergency and catastrophic situations. Threats can cause a variety of failures and failures, because the avionics of aircraft is very complex and saturated with complex computer networks.

The activity of civil aviation within the "ground-to-air" and "air-to-air" channels, the issue of safe operation of such aviation systems is becoming increasingly acute. In fact, each flight takes place in a complex network system, which includes a number of components: 1) the ground computer network of the airport and airlines, 2) the on-board computer network of the aircraft, 3) the network of information transmission between the communication methods of airport control points, aircraft (AC) and aeronautical systems for providing and controlling air traffic along the flight route.

Despite the fact that the risk of unauthorized interference is in each of the systems, which can create significant problems for aviation safety, the aviation data protection officer is primarily responsible for compliance with regulatory requirements and internal security regulations of the airport and airline ground computer network.

In the course of his work, the personal data protection officer is responsible for constantly reviewing and updating internal acts governing cybersecurity issues – both confidentiality agreements, trade secrets protection, and warnings regarding the processing of personal data regarding customers. The participation of this specialist is also required in the processes related to the remote work of the company's employees. Also among the tasks is the constant monitoring of the existing situation with the protection of personal data and taking measures to violate them.

References:

1. Illienko A., Illienko S., Kvasha D. (2020). Suchasnyi stan kiberbezpeky tsyvilnoi aviatsii ukrainy ta svitu [The current state of cybersecurity of civil aviation in Ukraine and the world]. Kiberbezpeka: osvita, nauka, tekhnika,

1(9), 24–36. https://doi.org/10.28925/2663-4023.2020.9.2436 [in Ukrainian].

2. Kobielieva T. (2020). Sutnist ta vyznachennia komplaiens-ryzyku [The essence and definition of compliance risk]. Visnyk Natsionalnoho tekhnichnoho universytetu “Kharkivskyi politekhnichnyi instytut” (ekonomichni nauky), 1. https://doi.org/10.20998/2519-4461.2020.1.116 [in Ukrainian].
3. Kovalenko S. (2021, 27 kvitnia). Osoblyvosti funktsii komplaiens v aviatsiinii haluzi [Features of the compliance function in the aviation industry]. Yurydychna hazeta online, 8 (738). https://yurgazeta.com/dumka-eksperta/osoblivosti-funkciyi-komplaens-v-aviaciyniy-galuzi.html [in Ukrainian].