УДК 004.056

Т.В. Кузнєцова, доцент,
А.В. Чирков
Національний авіаційний університет, Київ

STATE AND PERSPECTIVES OF AIRCRAFT CYBERSECURITY

During the latest events in the aviation world, where experts in the field of cybersecurity (example) opened the possibility of gaining access to the aircraft's on-board systems, industry experts (and not only) thought about it. And we are doing quite a lot. There are many existing guides that contain recommendations and practices, for example: «Software Considerations in Airborne Systems and Equipment Certification» contains recommendations for evaluating security and assuring software quality. There is a separation of access, because all systems are somehow connected to each other through the on-board network (take at least maintenance to determine failures) – as a fig. 1:

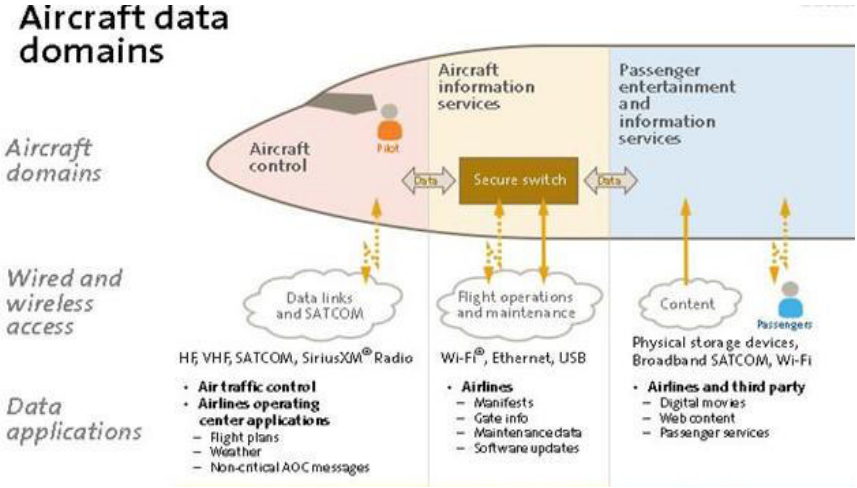

Fig. 1 Security and access restriction determined by aircraft domain [2]

• A high degree of integration of airborne equipment creates vulnerabilities in the security system;

• The FAA (US Federal Aviation Administration) did not properly implement the requirements for the Next Generation Air Transportation System (NextGen);

• An integrated information management network called SWIM based on satellite navigation of aircraft, tracking and digital transmission of voice and data creates significant and unresolved problems of cybersecurity;

• ADS-B technology, the introduction of which is planned to replace traditional radars, is inherently vulnerable to hacking due to its open architecture and the use of unencrypted signals.

GAO therefore highly recommended the FAA [1]:

• To fully apply the "Recommendations on information security throughout the life cycle of systems" developed by NIST (National Institute of Standards and Technology, also maintains a database of vulnerabilities);

• Make greater emphasis on guaranteeing the quality of airborne systems and consider safety and integrity issues in the airworthiness certification process.

The FAA continues to consider the aircraft guidelines acceptable for software certification, although they acknowledge that the guidelines do not fully cover all areas of software development and life cycle processes, and can sometimes be misinterpreted (Fig. 2).

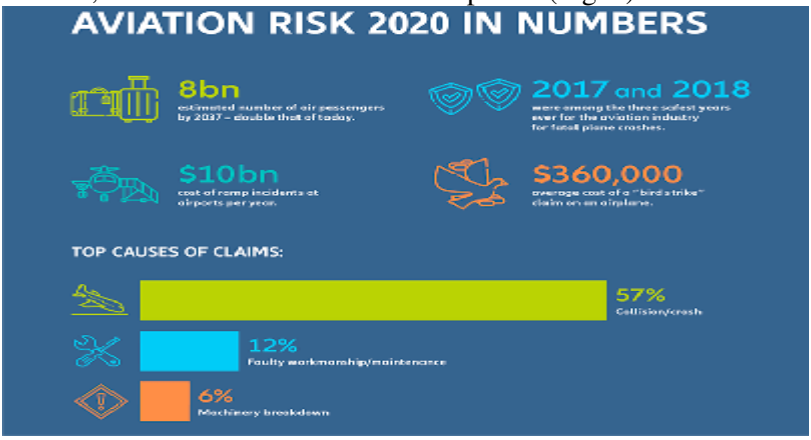

Fig. 2 Aviation Risk Forecast for 2020 [4]

Needless to say, the problem is finally recognized. She is, she exists. Some thought about it while watching the discovery movie «Inside A Plane Crash» – a Boeing crash test performed remotely. Some began to

breed panic and exposure. Nevertheless, at present, there is no single integrated approach to cybersecurity in the field of civil aviation. The American Institute of Aeronautics and Astronautics (AIAA) has published a general framework for aviation cybersecurity. The International Air Transport Association (IATA) has developed a set of cybersecurity tools. However, the FAA did not approve of them and set a goal to develop their own strategy that defines cybersecurity approaches to the entire aviation system. Actually, the work is being done in our aviation slowly, but with the deepest control and analysis of everything and everything, so that you can be calm and confident that you will fly in safety.

Although technology improves computer security, you should not forget about vigilance, for example, when receiving emails by e-mail. Hackers often hide behind messages from travel services, such as Airbnb, Booking.com, write on behalf of airlines, inform the user that they have paid for a plane ticket with their credit card, and offer a link to a phishing site where they allegedly can find out information about the upcoming flight [3].

In October 2019, it was the turn of cybercriminals who used the hype around the Ebola virus to send malicious emails. Again, WHO was indicated as the sender. In the text of the letters discovered by the experts, the attackers tried to convince the recipient that WHO had prepared a file with general information and precautions that would help protect the user and others from the deadly virus and other diseases.

In addition to exploiting topics that are relevant to society, spammers also send fake receipts from online stores invoicing a completed purchase, which can only be canceled on the phishing site [5].

REFERENCES

1. https://www.rbc.ua/ukr/tag/hakery
2. https://www.rbc.ua/ukr/tag/kiberataka
3. https://www.ukrinform.ru/tag-kiberataka
4. https://slovoidilo.ua/2020/04/13/kolonka/aleksandr-radchuk/bezopasnost/poligon-xakerskix-diversij-chto-zhdet-ukrainu-eru-kibervojn
5. https://forinsurer.com/news/20/04/10/37499