UDC 629.735.015.7.2:656.7.08(045)
DOI:10.18372/1990-5548.75.17563

[1]D. O. Shevchuk,
[2]I. A. Steniakin

A HOLISTIC APPROACH TO ENSURING SAFETY AND CYBERSECURITY IN THE USE OF INTELLIGENT TECHNOLOGIES IN AIR TRANSPORT

Department of Air Transport Organization, Faculty of Transport, Management and Logistic,
National Aviation University, Kyiv, Ukraine
E-mails: [1]dmitroshevchuk@gmail.com ORCID 0000-0001-9911-7214,
[2]ivansteniakin@gmail.com ORCID 0000-0002-3511-6826

Abstract*—The article is devoted to the study and analysis of the problems associated with the use of intelligent technologies in air transport security and cybersecurity issues. Possible dangers that may arise when using autonomous systems, including autonomous aircraft, are considered. The technical measures that can be taken to prevent these dangers, including the development of new methods of cybersecurity and protection against hacker attacks, are analyzed. The problem of ensuring security in air transport associated with the introduction of new technologies and automated systems is investigated. The risks associated with this process are described, such as possible aircraft accidents, data storage problems, and passenger safety issues. Technical measures that can be taken to ensure safety in air transport, including the development of new technologies and diagnostic methods that can detect possible problems before they become serious, are considered. Practical solutions to these problems are proposed, including the development of new security and cybersecurity systems that can be used in air transport. The technical measures that can be taken to ensure the safety and efficiency of the use of intelligent technologies in air transport are described. It is established that the developed simulation model can serve as an effective tool for managing the processes of aircraft ground handling at the airport, as well as allow predicting the results of such processes and developing algorithms for the rational allocation of resources, considering the functioning of the system in different modes. To ensure the efficient functioning of the aircraft ground handling system, it is proposed to implement technical measures to improve cybersecurity and ensure the system's resilience to possible cyberattacks.*

Index Terms—Air transport; artificial intelligence; machine learning; decision-making systems; cybersecurity; framework; intelligent technologies; encryption.

I. INTRODUCTION

Intelligent technologies, such as artificial intelligence (AI) and machine learning (ML), are rapidly changing the air transport industry. These technologies have the potential to revolutionize the way we travel, making air travel safer, more efficient, and more convenient. However, there are also some problems associated with the use of these intelligent technologies in air transport. In this article, we will explore some of the main problems of intelligent technologies on air transport.

Safety is the top priority in air transport, and the use of intelligent technologies must not compromise it. While AI and ML have the potential to enhance safety in air transport, they also raise new safety concerns. For example, AI-powered decision-making systems may make incorrect decisions due to data biases or errors in the algorithm. This could lead to unsafe situations, especially if the system is controlling critical functions such as autopilot or collision avoidance.

The use of intelligent technologies in air transport also raises cybersecurity risks [1]. As aircraft become more connected and reliant on technology, they become vulnerable to cyber attacks. For example, hackers could gain access to an aircraft's system and take control of critical functions, such as the engines or flight controls. This could lead to a catastrophic accident, putting passengers and crew at risk.

As intelligent technologies become more prevalent in air transport, there is a risk that pilots and other aviation professionals may become over-reliant on them. This could lead to a degradation of skills, making it harder for them to handle situations when the technology fails or malfunctions. In addition, pilots may become less proficient in manual flying skills, which could lead to errors in critical situations.

Intelligent technologies require significant investment in research, development, and implementation. While they have the potential to save costs in the long term, the initial investment can be a significant burden for airlines. This could lead to a widening gap between larger airlines that can afford to invest in these technologies and smaller airlines that cannot.

II. Problem Statement

Intelligent technologies, such as AI and IoT, are increasingly being used in air transport to improve safety and efficiency. However, these technologies also introduce new safety and cybersecurity risks that need to be addressed. The use of intelligent technologies in air transport requires careful consideration of these risks and the implementation of appropriate technical and organizational measures to ensure safety and security.

III. Problem Solution

Safety concerns in air transport are critical issues that can have serious consequences for passengers, crew, and the wider aviation industry. The increasing use of intelligent technologies, such as artificial intelligence (AI) and machine learning (ML), in air transport (Fig. 1) has raised several safety concerns that need to be addressed to ensure the safety of air travel [2].

One safety concern related to the use of intelligent technologies is the potential for biases or errors in the algorithm used to make decisions. For example, an AI-powered decision-making system may use biased data to make decisions, which could result in incorrect decisions that compromise safety [3]. Similarly, errors in the algorithm used to make decisions could lead to unsafe situations, particularly if the system is controlling critical functions such as autopilot or collision avoidance.

Another safety concern related to the use of intelligent technologies is the potential for unintended consequences. For example, an AI-powered system that controls flight operations could make decisions that unintentionally lead to unsafe situations. These unintended consequences can be difficult to predict, and it is essential to have appropriate safeguards and human oversight in place to ensure that these systems do not compromise safety.

A third safety concern related to the use of intelligent technologies is the potential for skill degradation among pilots and other aviation professionals. As intelligent technologies become more prevalent in air transport, there is a risk that pilots and other aviation professionals may become over-reliant on them [4]. This could lead to a degradation of skills, making it harder for them to handle situations when the technology fails or malfunctions. In addition, pilots may become less proficient in manual flying skills, which could lead to errors in critical situations.

One of the key technical measures that can be implemented to ensure safety and cybersecurity in the use of intelligent technologies in air transport is the development of secure and resilient systems. Intelligent information systems are characterized by ability to work with uncertain and dynamic data [5]. This involves designing systems that are resistant to cyber attacks and other forms of interference. Additionally, regular testing and auditing of these systems should be conducted to identify and mitigate vulnerabilities.

One of the key technical measures for ensuring safety and cybersecurity is the development of secure and resilient systems. This involves designing systems that are resistant to various cyber attacks (Fig. 2) and other forms of interference. To achieve this, a number of different techniques can be used, including encryption, access controls, and intrusion detection.

Encryption is a technique for protecting data from unauthorized access [6]. It involves transforming data into a coded form that can only be deciphered using a secret key. In air transport, encryption can be used to protect data transmitted between different systems, such as aircraft systems and ground control systems. The effectiveness of encryption can be quantified using mathematical algorithms, such as the Advanced Encryption Standard (AES), which is widely used in the aviation industry.

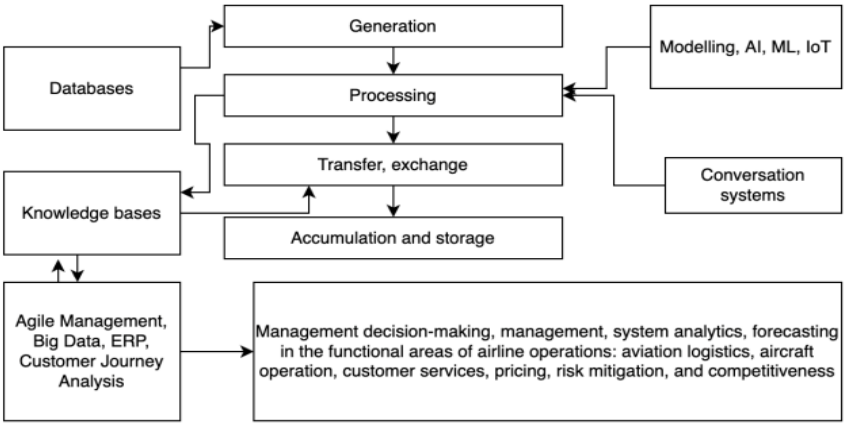

Fig. 1. Intelligent airline information systems structure

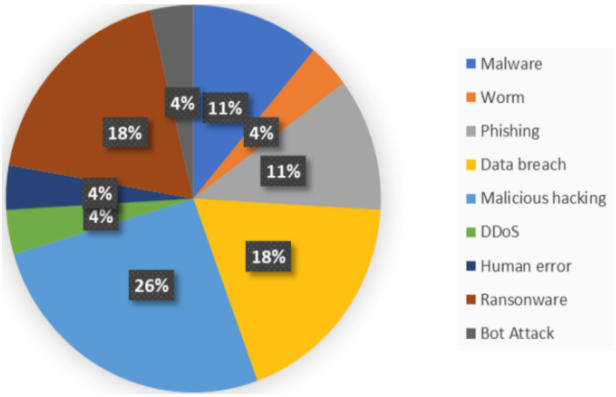

Fig. 2. Types of cyber-attacks in aviation industry

Access controls are used to restrict access to systems and data to authorized users only (Fig. 3). This can be achieved through the use of passwords, biometric identification, and other authentication mechanisms. The effectiveness of access controls can be measured using metrics such as the false acceptance rate (FAR) and false rejection rate (FRR), which are used to evaluate the accuracy of biometric identification systems [7].

Intrusion detection involves monitoring systems for signs of unauthorized access or other security breaches. This can be achieved through the use of software tools that analyze system logs and network traffic to identify potential threats. The effectiveness of intrusion detection can be measured using metrics such as the detection rate and false positive rate, which are used to evaluate the accuracy of intrusion detection systems.

Regular testing and auditing of systems is also an important technical measure for ensuring safety and cybersecurity in air transport [8]. This involves conducting regular penetration testing and vulnerability assessments to identify potential security weaknesses. The effectiveness of testing and auditing can be measured using metrics such as the number of vulnerabilities identified and the time taken to remediate these vulnerabilities.

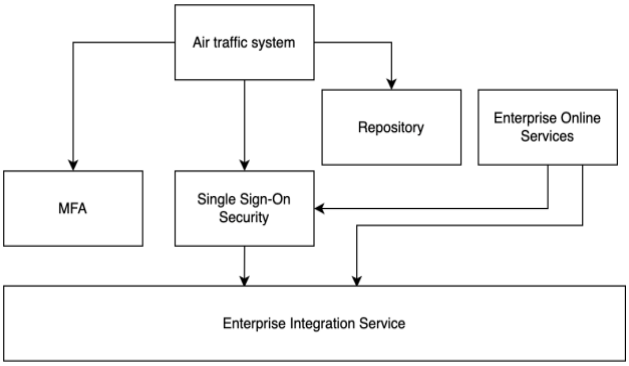

Fig. 3. Access controls enterprise pattern

Organizational measures can also be implemented to ensure safety and cybersecurity in the use of intelligent technologies in air transport. This includes ensuring that appropriate policies and procedures are in place to govern the use of these technologies [9]. Additionally, regular training and awareness programs should be provided to employees to help them detect and prevent potential security risks.

To mitigate these safety concerns, air transport organizations must implement appropriate safeguards and oversight mechanisms for the use of intelligent technologies. This includes ensuring that algorithms used in decision-making systems are regularly reviewed and audited for biases and errors. Additionally, air transport organizations must provide regular training and awareness to employees to help them detect and prevent unintended consequences and maintain their manual flying skills. Finally, air transport organizations must work with regulators and other stakeholders to ensure that appropriate legal and regulatory frameworks are in place to govern the use of intelligent technologies in air transport.

IV. Conclusion

The increasing use of intelligent technologies in air transport has the potential to transform the industry, but it also poses significant safety and cybersecurity risks. To ensure the safe and secure use of these technologies, a holistic approach that includes technical, organizational, and regulatory measures must be adopted. This approach will help to mitigate potential risks and ensure that the benefits of these technologies can be realized without compromising safety and security.

Intelligent technologies have the potential to revolutionize air transport, but they also raise several problems that need to be addressed. Safety concerns, cybersecurity risks, skill degradation, cost, and legal and regulatory challenges are some of the main issues that need to be tackled. Airlines, regulators, and other stakeholders must work together to ensure that the benefits of intelligent technologies in air transport are realized while mitigating their potential risks.

Technical measures play a critical role in ensuring the safety and cybersecurity of intelligent technologies in air transport. Techniques such as encryption, access controls, and intrusion detection can be used to develop secure and resilient systems, while testing and auditing can be used to identify and remediate potential security weaknesses. By using these measures in combination with organizational and regulatory measures, the aviation industry can ensure that the benefits of intelligent technologies can be realized without compromising safety and security.

REFERENCES

[1] International Air Transport Association. (2021). Global Aviation Data Management Report 2021. https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/iata-annual-review-2021.pdf

[2] A. Patterson, Information Systems – Using Information, Learning and Teaching Scotland, 2005.

[3] European Union Aviation Safety Agency. (2021). European Aviation Safety Plan 2021–2025. https://www.easa.europa.eu/en/document-library/general-publications/annual-safety-review-2021

[4] National Institute of Standards and Technology. (2017). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[5] A. Biryukov, D. Khovratovich, & I. Nikolić, (2016). Distinguisher and related-key attack on the full AES-256. In Advances in Cryptology – CRYPTO 2016 (pp. 1–20). Springer.

[6] A. K. Jain, A. Ross & K. Nandakumar, (2016). Introduction to biometrics. Springer.

[7] ISO/IEC 27001 Information technology – Security techniques – Information security management systems. (2013). https://www.iso.org/standard/54534.html

[8] European Union Agency for Cybersecurity. (2021). Good practices for securing smart airports. https://www.enisa.europa.eu/publications/securing-smart-airports

[9] National Cyber Security Centre. (2018). Penetration Testing: Technical Guide. https://www.ncsc.gov.uk/guidance/penetration-testing

Received February 02, 2023.

Shevchuk Dmitriy. ORCID 0000-0001-9911-7214.
Doctor of Engineering Science. Senior research scientist. Head of the Department of Air Transport Organization.
Faculty of Transport, Management and Logistic, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine, (2003).
Research area: methods of restoring the aircraft controllability in special situations in flight.
Publications: 128.
E-mail: dmitroshevchuk@gmail.com

Steniakin Ivan. ORCID 0000-0002-3511-6826. Post-graduate student. Software engineer.
Department of Air Transport Organization. Faculty of Transport, Management and Logistic, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine, (2021).
Research area: intelligent technologies in CRM systems.
E-mail: ivansteniakin@gmail.com

Д. О. Шевчук, І. А. Стенякін. Комплексний підхід до забезпечення безпеки та кібербезпеки при використанні інтелектуальних технологій на повітряному транспорті

Статтю присвячено дослідженню та аналізу проблем, пов'язаних зі застосуванням інтелектуальних технологій у повітряному транспорті, зокрема, проблем безпеки та кібербезпеки. Розглянуто можливі небезпеки, які можуть виникнути під час використання автономних систем, в тому числі автономних повітряних транспортних засобів. Проаналізовано технічні заходи, які можуть бути прийняті для запобігання цим небезпекам, включаючи розробку нових методів кібербезпеки та захисту від хакерських атак. Досліджено проблему забезпечення безпеки в повітряному транспорті, пов'язану з впровадженням нових технологій та автоматизованих систем. Описано ризики, пов'язані з цим процесом, такі як можливі аварії повітряних суден, проблеми зі збереженням даних та проблеми з безпекою пасажирів. Розглянуто технічні заходи, які можуть бути прийняті для забезпечення безпеки в повітряному транспорті, включаючи розробку нових технологій та методів діагностики, що дозволяють виявляти можливі проблеми до того, як вони стануть серйозними. Запропоновано практичні рішення для вирішення цих проблем, зокрема, розробка нових систем безпеки та кібербезпеки, які можуть бути використані в повітряному транспорті. Описано технічні заходи, які можуть бути прийняті для забезпечення безпеки та ефективності використання інтелектуальних технологій в повітряному транспорті. Встановлено, що розроблена імітаційна модель може слугувати ефективним інструментом управління процесами наземного обслуговування повітряних суден в аеропорту, а також дозволить прогнозувати результати таких процесів і розробляти алгоритми раціонального розподілу ресурсів з урахуванням функціонування системи в різних режимах. Для забезпечення ефективного функціонування системи наземного обслуговування повітряних кораблів запропоновано впровадження технічних заходів з покращення кібербезпеки та забезпечення стійкості системи до можливих кібератак.

Ключові слова: повітряний транспорт; штучний інтелект; машинне навчання; системи прийняття рішень; кібербезпека; фреймворк; інтелектуальні технології; шифрування.

Шевчук Дмитро Олегович. ORCID 0000-0001-9911-7214.
Доктор технічних наук. Старший науковий співробітник. Завідувач кафедри організації авіаційних перевезень.
Факультет транспорту, менеджменту і логістики, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна, (2003).
Напрям наукової діяльності: методи відновлення керованості літака в умовах виникнення особливих ситуацій у польоті.
Кількість публікацій: 128.
E-mail: dmitroshevchuk@gmail.com

Стенякін Іван Андрійович. ORCID 0000-0002-3511-6826. Аспірант. Асистент.
Кафедра організації авіаційних перевезень, Факультет транспорту, менеджменту і логістики, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна, (2021).
Напрям наукової діяльності: інтелектуальні технології у CRM системах.
E-mail: ivan.steniakin@gmail.com