phpMyAdmin, організовану файлову структуру та систему реєстрації, авторизації та профілю користувача.

Проєкт має гнучку архітектуру і може бути розгорнутий на будь-якому хостингу. Він стане ефективним інструментом у процесі професійної мовної підготовки студентів та учнів в умовах дистанційного навчання.

Окрему увагу при розробці було приділено зручності інтерфейсу та адаптивності системи до потреб різних категорій користувачів. Візуальні компоненти сайту реалізовані з урахуванням принципів доступності, що дозволяє ефективно взаємодіяти із системою як досвідченим користувачам, так і новачкам.

Система підтримує можливість розширення функціоналу, зокрема передбачено подальшу інтеграцію відеозв'язку, чатів, а також аналітики успішності користувачів. Це відкриває шлях до створення повноцінного цифрового навчального середовища, яке відповідатиме сучасним вимогам та стандартам освіти.

Висновки. Розроблений веб-застосунок демонструє ефективне поєднання сучасних технологій із педагогічними принципами контролю та зворотного зв'язку. Завдяки реалізації чіткої ролі викладача, гнучкому розмежуванню доступу та підтримці основних функцій навчального процесу, система дозволяє не лише підвищити якість дистанційного навчання, але й зробити його структурованим, інтерактивним і результативним. Запропонований підхід може бути адаптований для викладання інших дисциплін і сприяти подальшому розвитку цифрової освіти в Україні.

ENSURING CYBERSECURITY OF ATM SYSTEMS IN CIVIL AVIATION

Oliinyk Volodymyr
Ph.D. in Technical Sciences, Associate Professor
Department of automatic safety systems and information technologies
National University of Civil Defence of Ukraine, Ukraine
Oliinyk Elvira
Candidate for a Bachelor's degree
Department of Information Technology Security
Kharkiv National University of Radio Electronics, Ukraine

Abstract. The article discusses current issues of cybersecurity in civil aviation, in particular in air traffic management (ATM) systems. The main threats, such as spoofing, signal jamming and attacks on ground infrastructure, as well as their potential impact on flight safety are analysed. Special attention is paid to international and national regulations governing the protection of aviation systems.

Keywords: cybersecurity, civil aviation, air traffic management, ATM, cyber threats, normative documents.

Introduction. In today's world, civil aviation is a key link in the global transport system, ensuring the fast and safe movement of people and goods. It is a complex technological network that includes aircraft, airports, air traffic control, radar systems, computer databases and communication channels. All these elements actively interact with each other, making aviation infrastructure vulnerable to cyber threats. While the speed of information exchange and automation improve efficiency, they also create new opportunities for potential attacks. Vulnerabilities in these systems can lead to serious consequences, ranging from financial losses to threats to passenger lives. Therefore, the issue of cybersecurity in aviation is becoming increasingly relevant and requires a comprehensive approach.

Purpose and objectives of the study. The main purpose of the study is to identify the key risks of cyber threats in civil aviation air traffic control systems, as well as to analyse ways to ensure cybersecurity at the national and international levels. The study set the following objectives: to analyse the current regulatory framework in the field of aviation security; to study the statistics of cyber incidents in ATM systems; to identify potential infrastructure vulnerabilities; to consider recommendations of international organisations such as ICAO.

Research results and discussion. The study found that air traffic management (ATM) systems are extremely complex, interconnected and technologically advanced structures that are vulnerable to a wide range of cyber threats. Given the critical role they play in ensuring flight safety, any interference with such systems could have catastrophic consequences.

First of all, it is worth paying attention to the current regulatory framework. International organisations, including ICAO, have been emphasising the importance of integrating cybersecurity into the overall aviation security architecture since 2019. Documents such as Annex 17, Doc 9985, and the Global Aviation Security Plan provide specific guidance on how to protect ATM from cyber threats, especially in terms of wireless communications, navigation, and flight data processing. However, even the best standards can remain a formality without proper implementation. National authorities, including those in Ukraine, are gradually moving closer to European standards through harmonisation with EASA requirements, in particular with the introduction of Part-IS rules [1].

Real-life events of recent years demonstrate that the threat of cyberattacks on aviation is not abstract. For example, in 2018, British Airways suffered a serious attack that resulted in the theft of personal and financial data of more than 400,000 passengers [2]. The attacker penetrated the internal network through a compromised account of a company partner, which demonstrates the importance of access control and multi-factor authentication.

Even more alarming was the case in 2023, when pilots flying over the Black Sea reported massive GPS signal disruptions, allegedly caused by electronic warfare [3].

In some cases, navigation systems showed false coordinates, indicating spoofing, a type of attack where an attacker replaces real signals with fake ones, causing avionics to ‘see’ a different picture of the airspace.

In addition to GPS, spoofing can also affect ADS-B protocols, which automatically broadcast the aircraft's location [4]. Due to the lack of encryption and authentication, anyone with specialised equipment can not only listen to the transmitted data, but also broadcast fake data or change the coordinates of real vessels. Another common threat is signal jamming, where attackers block communication between aircraft and control centres. This is especially critical for GNSS systems and UHF/VHF communications, which do not have a sufficient level of protection against interference.

Ground-based infrastructure can also be attacked. Hacking into airport servers or ATM control centres can interfere with flight plans, make changes to schedules, or completely paralyse the work of air traffic control services. Such attacks are often combined with social engineering techniques, where hackers use phishing emails or manipulate staff to gain access to systems.

Among the possible security measures discussed both in scientific publications and in ICAO and EASA strategies, it is worth noting the need to introduce encryption and authentication for wireless communication protocols. It is also extremely important to raise the level of cyber awareness among aviation industry employees, as the human factor remains one of the weakest points. Another area is the development of backup navigation systems capable of operating in the event of a GNSS failure, as well as the creation of multi-level systems for real-time monitoring and anomaly detection.

Conclusions. The study showed that cybersecurity in civil aviation is a critical area, as vulnerabilities in ATM systems can have catastrophic consequences. Existing threats, such as spoofing, signal jamming and infrastructure attacks, require comprehensive solutions, including updating the regulatory framework, implementing modern security technologies and continuous risk monitoring. Implementation of these measures will reduce the likelihood of cyber incidents and ensure air transport safety.

References

1. European Union Aviation Safety Agency. (2025). Ukraine. EASA. https://www.easa.europa.eu/en/domains/international-cooperation/easa-by-country/countries/ukraine
2. Rodgers, Jason. (2021). British Airways Data Breach Claim Becomes Biggest Of Its Kind In The UK. Pogust Goodhead. https://pogustgoodhead.com/british-airways-data-breach-claim-becomes-biggest-of-its-kind-in-the-uk/
3. Safe Airspace. (2023). Conflict Zone & Risk Database. Safe Airspace. https://safeairspace.net/turkey/
4. Georgia Lykou. (2019). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies. Critical Infrastructure Security and Resilience, pp.245-260. DOI:10.1007/978-3-030-00024-0_13