Mirosław Karpiuk*
Miroslav Kelemen**

Cybersecurity in civil aviation in Poland and Slovakia

Abstract

Civil aviation, similar to other economy sectors, is exposed to cyber-attacks. In this case however, the protection against cybersecurity threats is gaining particular significance, as the industry relies heavily on the use of information systems (information and communication systems with electronic data processed in such systems). The systems are exposed to incidents. Incidents in civil aviation are events occurring in cyberspace which affect, or might potentially affect, the security of aircraft.

The issue of cybersecurity in civil aviation is discussed in the context of legal regulations that are in force in Poland and Slovakia. Individual solutions aimed at ensuring the cybersecurity of air transport were analysed.
Key words: civil aviation, air transport, cybersecurity, operator of essential services

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

** Prof. Miroslav Kelemen, PhD, Technical University of Kosice, Faculty of Aeronautics, e-mail: miroslav.kelemen@tuke.sk.

Introduction

Cyberspace is a place where activities are conducted in the public, private, social or economic spheres. It serves the purpose of providing various types of services and communication. It is of great significance for the state and society; therefore, both public and private institutions (primarily operators of essential services and digital service providers) have the responsibility to protect it. The protection against cyber threats should constitute a priority area of state policy, and an obligation on the part of entities responsible for the security of information systems.

Cyberspace should be properly protected, and the need results not only from the fact that it has a key significance for the functioning of public institutions, but also from the needs of an information society, extensively using various forms of communication[1].

According to the legal definition, cybersecurity is understood as the ability of information systems to resist action that compromises the availability, authenticity, integrity and confidentiality of processed data or the related services offered by those information systems[2]. Cybersecurity is also defined as the ability of networks and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by, or accessible via, those network and information systems[3].

1 M. Karpiuk, *The Organisation of the National System of Cybersecurity: Selected No.s*, „Studia Iuridica Lublinensia" 2021, no. 2, p. 241.

2 Art. 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2020, item 1369, as amended), further referred to as the NCSA.

3 Art. 4(2) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2016, L 194, p. 1). For additional information about cybersecurity, refer to: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *Activities of local government units in the scope of telecommunication*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, ibidem, no. 1; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity no.s for the municipalities in Hungary*, ibidem 2020, no. 2; I. Hoffman, M. Karpiuk, *The local*

The information society we are dealing with today is based on information and communications networks and systems which are susceptible to disruptions[4]. Given the above, competent authorities for ensuring cybersecurity must take coordinated action both to eliminate and prevent such disruptions.

Cybersecurity in civil aviation in Poland

The operators of essential services have a special status in the sphere of cybersecurity in civil aviation. The operator of essential services is an entity listed in the NCSA, having an organisational unit in the territory of the Republic of Poland, in respect of which a competent authority for ensuring cybersecurity has issued a decision on recognising the entity as an operator of essential services. The above definition is set out in Art. 5(1) of the NCSA[5].

In both the transport industry and the air transport sector, the following entities may have the status of an operator of essential services: 1) air carriers – air transport undertakings holding a valid operating licence or an equivalent[6]; 2) airport operators – entities which have been entered as operators in the civil airport register[7], performing for air carriers and other aircraft users one or more of the following categories of ground handling services: a) services in respect of on-ground administration and supervision, b) passenger service, c) luggage handling, d) freight and mail handling, e) ramp handling, f) aircraft handling, g) services in respect of supplying aircraft with fuel, h) aircraft maintenance services, i) services in respect of flight operations and crew administration activities, j) surface transport, k) services in respect of the in-flight supply of food and beverages (catering) – the services are listed

self-government's place in the cybersecurity domain. Examples of Poland and Hungary, ibidem 2022, no. 1; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, ibidem.

4 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, ibidem 2019, no. 1, p. 145.

5 See also K. Chałubińska-Jentkiewicz, *Komentarz do art. 5* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 71.

6 Art. 3(4) of the Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Official Journal of the European Union 2008, L 97, p. 72), further referred to as the EU Regulation.

7 Art. 2(7) of the Act of 3 July 2002 – the Aviation Law (consolidated text, Journal of Laws 2018, item 1183), further referred to as the AL.

in Art. 176 of the AL[8]; 3) regulated agents – air carriers, agents, freight forwarders or any other entities who ensure security controls in respect of cargo or mail (Art. 3(26) of the EU Regulation), performing security checks for air carriers; and 4) air navigation service providers operating in Polish airspace (subject to appointment and certification)[9].

The competent authority for ensuring cybersecurity issues a decision on recognising an entity as an operator of essential services (including entities representing the transport industry and the air transport sector), if the conditions specified in Art. 5(2) of the NCSA have been met, i.e., 1) the entity provides an essential service; 2) the provision of such service relies on information systems; and 3) an incident is likely to cause a severe disruption to the operator's provision of an essential service. The minister competent for transport is responsible for ensuring cybersecurity in the transport industry, excluding the water transport sector[10]. Therefore, it is the minister competent for transport that issues decisions on recognising an entity as an operator of essential services in respect of air transport entities.

The materiality thresholds defining the levels of disruption to essential services in air transport were set out by the legislator[11] separately for individual operators providing essential services, taking into account the specific nature of their business. The materiality thresholds include:

8 Under Art. 176 of the AL, the legislator defines users as air carriers and/or other aircraft users, J. Walulik, *Komentarz do art. 176* [in:] *Prawo lotnicze. Komentarz*, ed. M. Żylicz, Warszawa 2016.

9 The appointment and certification of air navigation service providers by competent state authorities are some of the measures which are used to guarantee that air navigation tasks are performed in line with the required standards of responsibilities and powers of air navigation services, with a view to reaching and maintaining a high uniform level of air navigation security, efficient and effective operations of the air transport system, and due protection of the general interest, W. Dzienkiewicz, *Komentarz do art. 127* [in:] *Prawo lotnicze*...

10 The minister competent for transport manages the government administration department of transport which includes, in particular, 1) the operation and development of transport infrastructure, including the construction, upgrade, maintenance and protection of airports and fees for using the infrastructure; 2) air traffic, and 3) passenger and freight air transport. The minister competent for transport supervises the President of the Civil Aviation Authority and the Polish Air Navigation Services Agency, as per Article 27 of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended).

11 Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and materiality thresholds of the disruptive effect of incidents on the provision of essential services (Journal of Laws 2018, item 1806).

1) air transport undertakings holding a valid operating licence or an equivalent (air carriers), providing essential services, a) as regards passenger air transport – the number of users relying on an essential service rendered by a given entity defined as the transport of at least 500 000 passengers a year, calculated on the basis of average statistical data for three years preceding the issue of a decision on recognising an entity as an operator of essential services, or in the event of entities operating for a period shorter than three years, on the basis of statistical data for two full years or one full year preceding the issue of a decision; b) as regards freight air transport – a market share of the entity rendering essential services amounting to at least 25% of the freight transport flights on the domestic market, calculated on the basis of average statistical data for three years preceding the issue of a decision on recognising an entity as an operator of essential services, or in the event of entities operating for a period shorter than three years, on the basis of statistical data for two full years or one full year preceding the issue of a decision; 2) entities entered as operators in the civil airport register (airport operators), providing essential services: as regards services supporting air transport operations rendered by airport operators – the number of users relying on an essential service provided by a given entity, defined as services provided to at least 500 000 passengers a year, calculated on the basis of average statistical data for three years preceding the issue of a decision on recognising an entity as an operator of essential services, or in the event of entities operating for a period shorter than three years, on the basis of statistical data for two full years or one full year preceding the issue of a decision or, in the event of new entities whose scope of activities are expected to meet the threshold requirements for being recognised as an operator of essential services, on the basis of the Master Plan[12]; 3) undertakings holding a licence for ground handling services and

12 Airport Master Plans, which constitute the development plans of a given airport, drawn up for a period no shorter than 20 years by airport operators, specify: 1) the area covered by the Plan, with the allowable dimensions of building structures and natural structures; 2) information about the planned development of air traffic (divided by scheduled and chartered operations and by general aviation, passenger transport and freight transport); 3) the concept for ensuring air navigation service providers; 4) the concept for the spatial development of areas around the airport, 5) information about traffic capacity, taking into account the current parameters (for existing airports) or future airport parameters (divided by parameters related to runways, taxiways, ramps, terminals, air space, and access routes to the airport), in relation to the expected traffic development and planned airport upgrades; 6) economic and financial information concerning, in particular, the current and planned ownership structure, the expected sources of funds for investment projects, current and

air carriers, agents, freight forwarders or other entities who ensure security controls in respect of cargo or mail, providing essential services: a) as regards support activities to air transportation performed by the undertaking with a regulated agent status – factors characteristic of a given sector, namely the performance of security checks of cargo and air mail together with the assignment of SPX, SCO and SHR status to cargo, and/or the provision of an electronic information transfer service, including the security status of a given mail item to be sent by air to its destination, b) as regards support services to air transport rendered by an undertaking holding the status of a handling agent – factors characteristic of a given sector, which means that the proper provision of other essential services at the airport relies on the services rendered by the handling agent, whereas the provision of such services by other entities is not possible; and 4) air navigation service providers in Polish airspace, providing essential services: as regards supporting services to air transport provided by an air navigation service provider – the geographical range related to an area affected by an incident covering the provision of services on the entire territory of the country; the entity's ability to maintain a sufficient level of the essential service, taking into account the availability of alternative methods of service provision, perceived as the lack of an alternative for a service provided, and of its provision by another service provider in the event of an incident; factors characteristic of a given sector, covering services provided in respect of at least 10 000 flights a year, notwithstanding the maximum take-off weight and the number of passenger seats in an aircraft, with the number of flights calculated as a sum of take-offs and landings, and as an average value for the preceding three years.

As per Art. 8 of the NCSA, operators of essential services (including the ones operating in the air transport sector) are obliged to implement a security management system within their information systems being used for the provision of essential services, which comprises: 1) the performance of regular risk assessments for the occurrence of incidents and risk management; 2) the implementation of relevant and proportional technical and organisational measures, taking into account state of the art, including: a) maintenance and safe operation of the information system, b) physical and environmental safety, taking into account access control, c) safety and continuity of the provision

expected profitability and liquidity of the entity, the planned amount of airport fees and revenues on that account, taking into account the total revenues of the entity; and 7) other matters selected by the airport operator, as per Art. 55(6) of the AL.

of services on which essential services depend, d) the implementation, documenting, and maintenance of action plans allowing the continuous and uninterrupted provision of essential services, and ensuring confidentiality, integrity, availability and authenticity of information, e) the covering of the information system being used for the provision of essential services by a continuous monitoring system; 3) the collection of information about cybersecurity threats and the vulnerabilities of information systems being used to provide essential services, 4) incident handling; 5) the use of preventive measures and measures to mitigate the effect of incidents on the security of the information system being used to render essential services, including a) the application of mechanisms ensuring the confidentiality, availability and authenticity of data processed in the information system, b) the assurance of software updates, c) protection against unauthorised modifications in the information system, d) immediate action following the identification of vulnerabilities or cybersecurity threats; and 6) the use of communication measures allowing proper and safe communication as part of the national cybersecurity system. The obligations imposed on the operators of essential services includes the following basic actions and processes: risk management and the introduction of relevant physical, technical and organisational safeguards on its basis; incident handling and an effective response to incidents; and the assurance of a safe communication channel as part of the national cybersecurity system[13]. The security management system within the information system being used for the provision of essential services is a core preventive instrument allowing the prediction of cyber threats. The obligation to have such a system in place has been imposed on the operators of essential services due to the need to ensure the protection of information systems against cyber-attacks hindering (or making impossible in certain circumstances) the provision of essential services via such systems (including in the air transport sector of the transport industry).

13 C. Kosikowski, *Komentarz do art. 8* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

Cybersecurity in civil aviation in Slovakia

The basic document for solving the problem in civil aviation in Slovakia is the legal norm „Act on Civil Aviation (Aviation Act) and on Amendments to Certain Acts" (Act no. 143/1998 Coll.). This Act regulates the operation of aircraft in the airspace of the Slovak Republic according to the rules of flight applicable to civil aviation, in the field of civil aviation competence and authorization of members of aviation personnel, competence of aircraft and other aeronautical products, aircraft register, establishment and operation of airports and aircraft ground facilities, performance of air transport, aviation works and other business in civil aviation, protection of civil aviation, competence of state administration bodies and imposition of sanctions.

According to section 2 of this Act, an act of unlawful interference means the communication of false information (in accordance with section 180b of the Criminal Code) or the interruption of information flows necessary for the performance of air traffic, resp. reporting false information which may endanger the safety of passengers, flight crew, or ground staff at the airport, public order at the airport, or the smooth operation of air operations. The protection of cyberspace airports and air traffic is therefore important.

The issue of cybersecurity in civil aviation in Slovakia finds support in the legal norm, which is the Act on Cyber Security and on Amendments to Certain Acts of 30 January 2018. The law was approved by the National Council of the Slovak Republic.

The Act transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016[14] on measures to ensure a high level of security of networks and information systems in the Union into the conditions of Slovakia. It regulates the rights and obligations of persons as well as the authority and competence of public authorities by setting minimum requirements for the standard provision of important information systems in the Slovak Republic. It lays down minimum requirements for ensuring cyber security in this Act and does not prevent the application of stricter security measures. The main goal is the protection and functionality of cyberspace.

In relation to civil aviation, within the organization of state administration bodies according to § 4 letter a) b) Ministry of Transport and Construction

14 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high level of security of networks and information systems in the Union (Official Journal of the European Union 2016, L 194, p. 1).

of the Slovak Republic. The Transport Office of the Slovak Republic performs this key role on behalf of the Ministry. Due to coordination, another important body of state administration in the field of aviation is the Ministry of Defense, which is responsible for the activities of the Air Force of the Armed Forces of the Slovak Republic. The cooperating state administration body is also the Ministry of the Interior of the Slovak Republic, which is responsible for the operation of the Squadron of the Ministry of the Interior (the so-called government squadron).

The state uses the Unified Cyber Security Information System, defined in § 8. The system serves for the management, coordination, registration and control of the performance of the state administration in the field of cyber security and CSIRT units – Computer Security Incident Response Team. The number of users connected to the Internet has grown dramatically in the last few years. However, their awareness in the field of information security is different, and this creates space for computer incidents, which may ultimately affect the very operation of the state. What's more, there is still a low probability that a potential attacker will be discovered. Given the above facts, it is important that the digital space of the Slovak Republic (resp. NIKI – National Information and Communication Infrastructure) is protected and potential incidents are resolved, their consequences mitigated or eliminated.

The main task of the specialized unit CSIRT.SK is to solve information and security incidents in the Slovak Republic in cooperation with owners and operators of affected parts of NIKI, telecommunications operators, Internet service providers and possibly other state authorities (eg police, investigators, courts). Furthermore, building and expanding public knowledge in selected areas of information security and cooperation with foreign sister organizations and the representation of the Slovak Republic in the field of information security at the international level[15]. In order to coordinate national activities aimed at preventing and addressing ICT security issues, the international organization FIRST (Forum of Incident Response and Security Teams) was established in 1990, currently bringing together more than 180 CSIRT/CERT teams from around the world, of which members are: teams from government, commercial and academia. At European level, there is a TF-CSIRT group that facilitates the cooperation of CSIRT teams within Europe.

15 CSIRT.SK Available on Internet: https://www.csirt.gov.sk/index.html?csrt=8058637170998233146.

The TF-CSIRT provides a space for the exchange of experience and knowledge in the field of information security, works on the development of common standards and procedures for responding to security incidents and also helps in the creation of new CSIRT teams. Furthermore, the European Union Agency for Network and Information Security ENISA was established in 2004, which ensures coordination and methodically assists in building new CSIRT teams or developing existing teams.

The unified information system of cyber security consists of a public and a non-public part – a public part with content according to § 8 available on the portal of the National Security Office of the Slovak Republic, access to it is free of charge and takes place in real time. The law focuses primarily on the basic service, which means a service included in the list of basic services (including air transport) and depends on networks and information systems and is performed in at least one sector or sub-sector.

In the Transport sector, in the Air transport subsector, the basic services are: 1) air carriers – an air carrier with a valid operating license or equivalent; 2) airport managing bodies – an entity which, in connection with or without other activities, has, as the case may be, national laws, regulations or treaties to manage and control the airport infrastructure or airport network and to coordinate and control the activities of individual operators at the airports concerned; in the relevant airport networks, airports, including major airports, and entities operating ancillary facilities located at airports; 3) operators providing air traffic control (ATC) services as a service provided for purposes: a) collision avoidance – between aircraft, and – in the operating area between the aircraft and obstacles, b) and accelerating and maintaining the proper flow of air traffic; 3) administrators and operators of networks and information systems, which are an element of critical infrastructure according to Act no. 45/2011 Coll. critical infrastructure or are directly connected to it. Basic service is an element of the state's critical infrastructure.

In connection with the Transport sector, we must also mention the Water and Atmosphere sector, where the Aeronautical Meteorological Service operates within the Meteorological Service, i. administrators and operators of the state hydrological network; administrators and operators of networks and information systems, which are an element of critical infrastructure according

to Act no. 45/2011 Coll.[16] critical infrastructure or are directly connected to it; and administrators and operators of the state meteorological network.

The following impact criteria apply to the basic service: number of users using the basic service, dependence of other sectors of the basic service, the impact that cyber security incidents could have in terms of scale and duration on economic and social activities and state or national security interests, market share geographical distribution in terms of the area that could be affected by the cyber security incident, the importance of the basic service operator in terms of maintaining continuity of service.

The sector-specific criteria for the air transport sector, including airports and air carriers, rail transport and seaports, determine the specific criterion: the share of national transport and the number of passengers or freight operations per year. In accordance with § 17 the service provider notifies the state authority that the criteria have been exceeded within 30 days of the finding.

A cyber incident in civil aviation networks is any event which, due to a breach of network and information system security or a breach of security policy or binding methodology, has a negative impact on cyber security or results in loss of data confidentiality, destruction of data or breach of system integrity, restriction or denial of the availability of the basic service or digital service, a high probability of compromising the activities of the basic service, or a threat to information security. Cyber security incidents are reported in accordance with section 24 of the Act.

A cyber security incident is identified as a serious cyber security incident if it meets at least one identification criterion for the category of a serious cyber incident – specified in the draft decree. We recognize 3 categories of serious cyber security incidents: level I category; category II; category III.

For the identification criterion, the number of basic or digital service users affected by a cyber security incident is a limit of 15 000 for category I, 35 000 for category II, and 50 000 for category III.

For the identification criterion, the duration of a cyber security incident according to the percentage of time specified in the service level rules, which belong to individual services, the limit is more than 40% of the time for

16 Act no. 45/2011 Coll. on state critical infrastructure (Zbierka zákonov Slovenskej republiky 2011, 45, Vyhlásené znenie), https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/vyhlasene_znenie.html [access: 16.08.2022].

category I, more than 60% of the time for category II, More than 75% of time for category III.

For the identification criterion of the geographical spread of a cyber security incident, the limit is at least a district for category I, at least a region for category II, the whole Slovak Republic for category III.

For the identification criterion, the degree of disruption of the basic service or digital service, the limit is „partial" for category I, „complete" for category II, „complete without compensation" for category III.

For the identification criterion, the extent of the impact of a cyber security incident on the economic or social activities of the state is the limit of economic loss, the number of injured (dead), and the impact on public order.

An important agenda in ensuring cyber security in the field of civil aviation is the audit. The State Office (National Security Office of the Slovak Republic) may at any time carry out a cyber security audit of the basic service operator or request a conformity assessment body to carry out such an audit of the basic service operator in order to confirm the effectiveness of security measures taken and compliance with the requirements of this Act.

The personnel within the air transport ecosystem work in different workplaces, in different job positions. Individual human-caused failures, workflow incidents or technology failures in one section of airport information systems may jeopardize the integrity and security of the entire air traffic support system. For this reason, students are already preparing in three levels: general aviation education, training of aviation specialists and training using virtual training and information, simulation and communication technologies in the aviation environment. The proposed model makes it possible to divide students, future airport staff, into the following basic groups: security and safety, airline/airport management/operation, information technology (IT) and computers in aviation, and passenger management and services (air cargo and air passenger transport). For those interested in expanding knowledge and developing an academic and research discussion on civil aviation cyber security, we refer to our independent work on „Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport"[17]. There is currently no single method for developing risk management technologies by engaging expertise through an adaptive approach. An expert model for assessing airport NIS

17 M. Kelemen et al., *Educational model for evaluation of airport NIS security for safe and sustainable air transport*, „Sustainability" 2020, vol. 12, no. 16.

risks and incidents using fuzzy sets is an urgently needed task to improve civil aviation information security.

In the next period, the attention of the aviation community will be focused on the amendment to the Civil Aviation Act, which will also have an innovative impact on strengthening safety in civil aviation networks. Among other things, the legislator plans to establish a register of operators of unmanned aerial systems and unmanned aerial vehicles whose project proposal is subject to registration. In this agenda, Slovakia is only catching up with the other member states of the European Union. Flight safety is affected by the increase in drone activities near airports, both in controlled and uncontrolled airspace. The legal environment needs to strengthen tools against those who threaten air traffic safety and coordination, information security for the management, monitoring, transmission and sharing of data for the coordination of aircraft operations and unmanned aerial vehicles. In addition to civil air operations, the Act also applies, to a limited extent, to the operation of aircraft in military services, police services, customs services or flights in the public interest in the airspace, with the appropriate designation or note in the flight plan. This agenda requires increased protection of information and some of it is subject to a special confidentiality regime from unauthorized persons.

The issue of cyber security of civil air traffic raises many praxeological issues at a time of dynamic technological development and human error, which must be addressed at the national and international level of cooperation and coordination.

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity no.s for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2.

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Karpiuk M., *The Organisation of the National System of Cybersecurity: Selected No.s*, „Studia Iuridica Lublinensia" 2021, no. 2.
Kelemen M. et al., *Educational model for evaluation of airport NIS security for safe and sustainable air transport*, „Sustainability" 2020, vol. 12, no. 16.
Prawo lotnicze. Komentarz, ed. M. Żylicz, Warszawa 2016.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Cyberbezpieczeństwo w lotnictwie cywilnym w Polsce i na Słowacji

Streszczenie

Lotnictwo cywilne, podobnie jak i inne sfery gospodarki, jest narażone na cyberataki, w tym jednak przypadku ochrona przed zagrożeniami cyberbezpieczeństwa nabiera szczególnego znaczenia, ponieważ w tej branży na szeroką skalę wykorzystuje się systemy informacyjne (systemy teleinformatyczne wraz z przetwarzanymi w nich danymi w postaci elektronicznej). Systemy te narażone są na incydenty. Incydenty w lotnictwie cywilnym, będące zdarzeniami występującymi w cyberprzestrzeni, które mają lub mogłyby mieć wpływ na bezpieczeństwo statków powietrznych.

Problematyka cyberbezpieczeństwa w lotnictwie cywilnym omawiana jest na gruncie regulacji obowiązujących w Polsce i na Słowacji. Analizie poddano poszczególne rozwiązania, które w tych państwach mają zapewnić cyberbezpieczeństwo transportu lotniczego.

Słowa kluczowe: lotnictwo cywilne, transport lotniczy, cyberbezpieczeństwo, operator usługi kluczowej