Edyta SZCZEPANIUK
Lotnicza Akademia Wojskowa
e-mail: e.szczepaniuk@law.mil.pl
ORCID: 0000-0002-6707-2987

DOI: 10.55676/asi.v3i1.32

WYBRANE ASPEKTY CYBERBEZPIECZEŃSTWA W LOTNICTWIE CYWILNYM

SELECTED ASPECTS OF CYBERSECURITY IN CIVIL AVIATION

Streszczenie

Lotnictwo cywilne jest jednym z najważniejszych elementów globalnej infrastruktury transportowej, który odgrywa kluczową rolę w transporcie pasażerów i towarów. Rozwój nowych technologii i aktualne kierunki transformacji cyfrowej sprawiają, że coraz więcej obszarów lotnictwa cywilnego jest krytycznie uzależnionych od bezpiecznego funkcjonowania systemów informatycznych. Zależności te zwiększają ryzyko cyberataków, które mogą prowadzić do poważnych konsekwencji dla sektora lotniczego i bezpieczeństwa pasażerów. W związku z tym, cyberbezpieczeństwo jest jednym z kluczowych wyzwań dla lotnictwa cywilnego oraz stanowi istotne zagadnienie badawcze. Celem artykułu było przedstawienie problematyki cyberbezpieczeństwa w lotnictwie cywilnym, z uwzględnieniem zagrożeń, regulacji prawnych oraz wymagań krajowego systemu cyberbezpieczeństwa RP. Na potrzeby realizacji przyjętego celu wykorzystano analizę i syntezę literatury przedmiotu, aktów prawnych oraz danych statystycznych. Wyniki badań dowodzą, że cyberbezpieczeństwo w lotnictwie cywilnym jest zagadnieniem interdyscyplinarnym, które wymaga podejścia systemowego i uwzględnienia aspektów bezpieczeństwa i ochrony. W artykule zaproponowano klasyfikację zagrożeń dla cyberbezpieczeństwa w lotnictwie cywilnym, która może być rozwijana zarówno w obszarze eksponowanych zagrożeń, jak i dodatkowych kryteriów podziału. Analiza danych statystycznych wykazała, że w ostatnim czasie zwiększyła się ilość naruszeń danych, ataków *ransomware* i ataków DDoS na lotnictwo cywilne. W związku z rosnącym ryzykiem cyberataków podjęto szereg działań na rzecz cyberbezpieczeństwa. W artykule zaprezentowano ramy prawne cyberbezpieczeństwa w lotnictwie cywilnym, które obejmują regulacje międzynarodowe, regionalne i krajowe. Przy czym, kluczowe są również dokumenty strategiczne, normy, standardy i rozwiązania branżowe. Lotnictwo cywilne jest także elementem krajowego systemu cyberbezpieczeństwa RP, co determinuje konieczność realizacji określonych wymagań przez zaangażowane podmioty.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, krajowy system cyberbezpieczeństwa, lotnictwo cywilne, ramy prawne

Abstract

Civil aviation is one of the most important elements of the global transport infrastructure, which plays a crucial role in transporting passengers and goods. The development of new technologies and current directions in digital transformation mean that an increasing number of areas within civil aviation are critically dependent on the secure functioning of computer systems. These dependencies increase the risk of cyberattacks, which can lead to serious consequences for the aviation sector and passenger safety. Therefore, cybersecurity is one of the significant challenges for civil aviation and is an important research topic. The article aims to present the issues of cybersecurity in civil aviation, taking into account the threats, legal framework, and requirements of the national cybersecurity system of the Republic of Poland. In order to achieve the adopted research objective, the analysis and synthesis of the literature on the subject, legal acts, and statistical data were used. The research results prove that cybersecurity in civil aviation is an interdisciplinary issue that requires a systemic approach and considers both safety and security aspects. The article proposes a classification of threats to cybersecurity in civil aviation, which can be developed both in the area of exposed threats and additional division criteria. Statistical data analysis has shown that recently there has been an increase in the number of data breaches, ransomware attacks, and DDoS attacks on civil aviation. Due to the growing risk of cyberattacks, a number of cybersecurity measures have been taken. The paper presents the legal framework of cybersecurity in civil aviation, which includes international, regional, and national regulations. Strategic documents, norms, standards, and industry solutions are also of key importance. Civil aviation is also an element of the national cybersecurity system of the Republic of Poland, which determines the need to meet specific requirements by the entities involved.

Keywords: cybersecurity, cyberthreats, national cybersecurity system, civil aviation, legal framework

Artykuł wpłynął do redakcji: 14.06.2023 / Zatwierdzono do publikacji: 20.06.2023

1. WSTĘP

Rozwój nowych technologii i transformacja cyfrowa stanowią jeden z priorytetów wielu państw i organizacji międzynarodowych. Informatyzacja stwarza znaczące możliwości w zakresie rozwoju nowoczesnych sektorów gospodarki i usprawnienia procesów biznesowych w organizacjach. Opisywane trendy są także widoczne w sektorze lotniczym, który dynamicznie rozwija się w wyniku rosnącego popytu na usługi lotnicze oraz postępującej automatyzacji i cyfryzacji. Mając na uwadze aktualne kierunki transformacji cyfrowej, można przypuszczać, że w najbliższych latach coraz więcej obszarów lotnictwa cywilnego będzie krytycznie uzależnionych od bezpiecznego funkcjonowania systemów teleinformatycznych.

Analiza globalnego środowiska bezpieczeństwa pozwala dostrzec tendencje rozwojowe cyberzagrożeń dla lotnictwa cywilnego. Na problem ten zwróciła uwagę Europejska Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), która w raporcie dotyczącym incydentów cybernetycznych opublikowała dane o zagrożeniach w branży lotniczej za lata 2021–2022[1]. Odnosząc się do lat wcześniejszych, Europejska Organizacja ds. Bezpieczeństwa Żeglugi Powietrznej (EUROCONTROL) podała, że w 2020 r., liczba cyberataków w sektorze wzrosła o 530% w stosunku do roku poprzedniego[2]. Warto przy tym zaznaczyć, że cyberzagrożenia dla lotnictwa cywilnego mogą wpływać zarówno na jakość i efektywność świadczonych usług, jak i prowadzić do destabilizacji infrastruktury krytycznej oraz stanowić zagrożenie dla życia i zdrowia ludzi.

Współcześnie wiele instytucji, państw i organizacji dostrzega potrzebę intensyfikacji działań na rzecz cyberbezpieczeństwa. Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) podjęła inicjatywy w omawianym obszarze, do których można zaliczyć np. opracowanie Strategii Cyberbezpieczeństwa Lotnictwa[3] oraz Planu działań w zakresie cyberbezpieczeństwa[4]. Problematyka ta znalazła się także w obszarze zainteresowań Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA), która opracowała harmonogram działań na rzecz cyberbezpieczeństwa oraz zainicjowała powstanie Europejskiej Platformy Współpracy Strategicznej (ESCP) skupiającej interesariuszy branży lotniczej, przedstawicieli państw i instytucji Unii Europejskiej. Efektem tej współpracy było opracowanie europejskiej Strategii Cyberbezpieczeństwa w Lotnictwie[5]. Z zarysowanego kontekstu wynika, iż problematyka cyberbezpieczeństwa w lotnictwie cywilnym jest jednym z wyzwań sektora lotniczego, co uzasadnia potrzebę badań dotyczących niniejszej problematyki.

Celem artykułu było przedstawienie problematyki cyberbezpieczeństwa w lotnictwie cywilnym, z uwzględnieniem zagrożeń, regulacji prawnych oraz wymagań krajowego

1 Zob. „ENISA Transport Threat Landscape", ENISA, 2023, https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape [dostęp: 29.03.2023].
2 „Think Paper #12: Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?", EUROCONTROL EATM-CERT Services, 2021, https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf [dostęp: 29.03.2023].
3 Zob. „Aviation Cybersecurity Strategy", ICAO, October 2019.
4 Zob. „Cybersecurity Action Plan", ICAO, January 2022.
5 Zob. „Strategy for Cybersecurity in Aviation", ESCP, First Issue, September 2019.

 DOI: 10.55676/asi.v3i1.32

systemu cyberbezpieczeństwa RP. Na potrzeby realizacji przyjętego celu wykorzystano analizę i syntezę literatury przedmiotu, aktów prawnych oraz danych statystycznych.

2. ISTOTA CYBERBEZPIECZEŃSTWA W LOTNICTWIE CYWILNYM

Według ICAO cyberbezpieczeństwo obejmuje zbiór technologii, kontroli i środków oraz procesów i praktyk zaprojektowanych w celu zapewnienia poufności, integralności, dostępności, a także ogólnej ochrony systemów, sieci, programów, urządzeń, informacji i danych przed atakiem, uszkodzeniem, nieautoryzowanym dostępem, użyciem i/lub eksploatacją[6]. W przywołanej definicji zwrócono uwagę na rozwiązania proceduralno-organizacyjne, teleinformatyczne i fizyczne ukierunkowane na zapewnienie atrybutów bezpieczeństwa informacji oraz ochronę przed zagrożeniami.

Problematyka cyberbezpieczeństwa w lotnictwie cywilnym wymaga kompleksowego podejścia uwzględniającego następujące aspekty:

1. Akty prawne, dokumenty strategiczne, normy i standardy – prawo powszechnie obowiązujące ma kluczowe znaczenie, ponieważ określa ramy prawne oraz wymagania w zakresie cyberbezpieczeństwa. Dokumenty strategiczne wskazują wizję, priorytety i perspektywy rozwoju lotnictwa cywilnego w aspekcie ochrony przed cyberzagrożeniami. Natomiast normy i standardy ujednolicają dobre praktyki, które mogą przyczynić się do zwiększenia poziomu cyberbezpieczeństwa w lotnictwie cywilnym. Mając na uwadze powyższe, istotne jest, aby regulacje odpowiadały aktualnym i przyszłym wyzwaniom w zakresie cyberbezpieczeństwa w sektorze lotniczym.
2. Systemy i urządzenia wykorzystywane w lotnictwie cywilnym – są to rozwiązania o krytycznym znaczeniu dla operacji lotniczych, zarządzania portami lotniczymi oraz zapewniają łączność, przetwarzanie i udostępnianie danych między poszczególnymi podmiotami i systemami. Obejmują one m.in. systemy zarządzania ruchem lotniczym, systemy nawigacyjne oraz systemy informatyczne dedykowane dla pasażerów, takie jak np. systemy rezerwacji biletów lotniczych. Elementy te mogą być obiektem cyberataków, stąd też istotne znaczenie ma analiza ich podatności, zarządzanie ryzykiem i wdrożenie rozwiązań minimalizujących ryzyko. W literaturze przedmiotu wskazuje się także trendy technologiczne, jak np. inteligentne porty lotnicze[7]. Koncepcja ta bazuje głównie na technologii IoT, która posiada wiele problemów związanych z bezpieczeństwem[8]. W związku z tym, zagadnienie to wymaga intensyfikacji badań naukowych.

[6] Zob. „Cybersecurity Action Plan", dz. cyt.

[7] Zob. J. Thums, L. Künzel, M. Klumpp, M. Bardmann, C. Ruiner, *Future air transportation and digital work at airports – Review and developments*, „Transportation Research Interdisciplinary Perspectives" 2023, nr 19, https://doi.org/10.1016/j.trip.2023.100808 [dostęp: 13.04.2023].

[8] Zob. N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, H. Janicke, *A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports*, „IEEE Access" 2020, nr 8, https://doi.org/10.1109/ACCESS.2020.3036728 [dostęp: 13.04.2023], s. 209802–209834; H. Szczepaniuk, E. Szczepaniuk, *Cybersecurity Management within the Internet of Things,* [w:] *IoT Security Paradigms and Applications Research and Practices*, red. S.K. Sharma, B. Bhushan, N.C. Debnath, Taylor & Francis, Boca Raton 2021, s. 25–41.

3. Polityki, procedury i zarządzanie bezpieczeństwem – lotnictwo cywilne jest złożonym systemem obejmującym wiele podmiotów, które powinny wdrożyć dedykowane procedury i rozwiązania w zakresie cyberbezpieczeństwa, odpowiednie do specyfiki prowadzonej działalności. Istotnym aspektem jest aktualizacja polityk i procedur oraz zapewnienie ich zgodności z przepisami prawnymi oraz wymaganiami bezpieczeństwa lotniczego, w tym z normami i standardami branżowymi. Do kluczowych rozwiązań wewnętrznych można zaliczyć np. dokumenty określające zasady kontroli dostępu, procedury zarządzania incydentami bezpieczeństwa oraz procedury zarządzania ryzykiem. Ponadto, w literaturze przedmiotu[9] oraz dokumentach[10] zwraca się uwagę na potrzebę włączenia zagadnień cyberbezpieczeństwa do koncepcji Zintegrowanych Systemów Zarządzania Bezpieczeństwem w lotnictwie cywilnym.
4. Zabezpieczenia fizyczne, techniczne i teleinformatyczne – podstawową funkcją zabezpieczeń jest minimalizowanie ryzyka zagrożeń oraz ograniczenie możliwości nieuprawnionego dostępu do budynków, pomieszczeń, urządzeń i systemów. Warto przy tym zaznaczyć, iż w wielu normach i standardach do zabezpieczeń zalicza się także omówione wcześniej rozwiązania proceduralno-organizacyjne oraz zagadnienia bezpieczeństwa osobowego będące przedmiotem dalszej charakterystyki[11]. Innymi słowy, poszczególne zabezpieczenia są wzajemnie komplementarne oraz implementowane łącznie zwiększają skuteczność ochrony przed zagrożeniami. Do przykładowych rozwiązań można zaliczyć: kontrolę dostępu, systemy detekcji ruchu, systemy IDS/IPS zabezpieczenia biometryczne oraz szyfrowanie danych i transmisji.
5. Czynnik ludzki – potrzeba zwiększenia świadomości i kompetencji w obszarze cyberbezpieczeństwa wynika z rosnącej liczby cyberataków wykorzystujących podatność czynnika ludzkiego na zagrożenia. W literaturze przedmiotu ukształtowało się pojęcie cyberhigieny, które odnosi się do zbioru zasad i zachowań zwiększających bezpieczeństwo użytkowników indywidualnych oraz mających pozytywny wpływ na organizacje[12]. Istotnym aspektem jest więc włączenie zagadnień cyberbezpieczeństwa do kultury bezpieczeństwa w organizacjach. ICAO podkreśla, że ustanowienie kultury cyberbezpieczeństwa, jako integralnej części kultury organizacji sprzyja poprawie ogólnych wyników w zakresie ochrony przed cyberzagrożeniami[13]. Kluczowym elementem w tym obszarze jest np. wdrożenie programów edukacyjnych, regularnych kursów i szkoleń dla pracowników[14].

---

9 Zob. M. Khatun, F. Wagner, R. Jung, M. Glaß, *Identification of Interface related Factors between Safety Management System and Cybersecurity Management System for Highly Automated Driving Vehicles,* [w:] *Proceedings of the 25th International Conference on Enterprise Information Systems*, red. J. Filipe, M. Śmiałek, A. Brodsky, S. Hammoudi, SciTePress, Prague 2023, s. 21–30.

10 Zob. „Krajowy Program Bezpieczeństwa w Lotnictwie Cywilnym", ULC, Warszawa 2020.

11 Zob. PN-EN ISO 27001:2017-06, „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania", PKN, Warszawa 2017.

12 E. Szczepaniuk, H. Szczepaniuk, *Analysis of cybersecurity competencies: Recommendations for telecommunications policy*, „Telecommunications Policy" 2022, nr 46(3), https://doi.org/10.1016/j.telpol.2021.102282 [dostęp: 13.04.2023].

13 „Cybersecurity Culture in Civil Aviation", ICAO, January 2022, https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf [dostęp: 2.04.2023].

14 M. Żmigrodzka, *Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century*, „Safety & Defense" 2020, nr 6(2), https://doi.org/10.37105/sd.73 [dostęp: 13.04.2023], s. 33–41.

 DOI: 10.55676/asi.v3i1.32

6. Współpraca międzynarodowa – lotnictwo cywilne jest jednym z najistotniejszych sektorów transportu międzynarodowego, który wymaga współpracy w zakresie cyberbezpieczeństwa między państwami, organizacjami i innymi podmiotami, jak np. linie lotnicze, porty lotnicze, dostawcy usług teleinformatycznych i ośrodki naukowo-badawcze. Przykładowo współpraca może obejmować opracowanie dokumentów strategicznych, standardów i innych regulacji, wymianę informacji i doświadczeń, współpracę operacyjną i koordynację działań, walkę z cyberprzestępczością oraz realizację wspólnych szkoleń, ćwiczeń i symulacji na potrzeby zwiększenia zdolności reagowania na incydenty.

Podsumowując, cyberbezpieczeństwo w lotnictwie cywilnym jest dziedziną interdyscyplinarną, która wymaga podejścia systemowego i uwzględnienia zarówno aspektów bezpieczeństwa (ang. *safety*), jak i ochrony (ang. *security*). Przy czym, środowisko bezpieczeństwa jest zmienne, stąd zasadne jest ciągłe doskonalenie istniejących rozwiązań i uwzględnienie dynamiki zagrożeń w cyberprzestrzeni. W literaturze przedmiotu podkreśla się, iż kluczowe w tym zakresie jest prowadzenie systematycznej oceny ryzyka cyberbezpieczeństwa w lotnictwie cywilnym, ponieważ umożliwia ono identyfikację zagrożeń i ocenę prawdopodobieństwa ich wystąpienia, a także ograniczenie ryzyka do poziomu akceptowalnego za pomocą zabezpieczeń[15]. Rozwój cyfryzacji i automatyzacji w lotnictwie cywilnym sprawia, że cyberbezpieczeństwo jest warunkiem zapewnienia dostępności i integralności operacji lotniczych oraz ochrony przed cyberzagrożeniami.

3. ZAGROŻENIA DLA CYBERBEZPIECZEŃSTWA W LOTNICTWIE CYWILNYM

W ustawie o krajowym systemie cyberbezpieczeństwa zagrożenie cyberbezpieczeństwa zdefiniowano jako „potencjalną przyczynę incydentu bezpieczeństwa”[16]. Natomiast pojęcie »incydent« oznacza „zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo”[17]. Biorąc pod uwagę charakterystykę przedstawioną w poprzedniej sekcji, można przyjąć, że zagrożeniem dla cyberbezpieczeństwa w lotnictwie cywilnym będzie każde zdarzenie, które narusza lub może naruszyć atrybuty bezpieczeństwa informacji systemów wykorzystywanych w lotnictwie cywilnym, w tym także dane i usługi oferowane przez te systemy.

Zagrożenia dla cyberbezpieczeństwa w lotnictwie cywilnym obejmują szerokie spektrum zjawisk, które mogą być przyczyną incydentów bezpieczeństwa. W związku z ich złożoną specyfiką w tabeli 1 zaproponowano klasyfikację zagrożeń dla cyberbezpieczeństwa w lotnictwie cywilnym. Typologia obejmuje różne kryteria podziału i przykłady zagrożeń, a także referencje do przykładowych publikacji odnoszących się do wymienionych zagrożeń dla cyberbezpieczeństwa w lotnictwie cywilnym.

[15] A.A. Elmarady, K. Rahouma, *Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment*, „IEEE Access” 2021, nr 9, https://doi.org/10.1109/ACCESS.2021.3121230 [dostęp: 13.04.2023], s. 143997–144016.

[16] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

[17] Tamże.

Tabela 1 nie wyczerpuje problematyki klasyfikacji zagrożeń dla cyberbezpieczeństwa w lotnictwie cywilnym, ale obejmuje wybrane ich przykłady wyszczególnione w oparciu o różne kryteria podziału. Zagrożenia mogą być przykładowo analizowane także według: skutków[18], aktorów zagrożeń[19], wybranych modeli (np. metodyka ATT&CK MITRE[20]) lub konkretnych urządzeń i systemów lotnictwa cywilnego[21]. Warto przy tym zaznaczyć, że zastosowanie konkretnej typologii jest determinowane w szczególności celem prowadzonej identyfikacji oraz specyfiką organizacji i stosowanych w niej systemów. Ogólnie można przyjąć, iż identyfikacja zagrożeń jest niezbędnym elementem zarządzania ryzykiem, wspomaga podejmowanie decyzji w zakresie wyboru odpowiedniej strategii ochronnej, sprzyja rozpoznaniu podatności urządzeń i systemów, wpływa na kształtowanie kultury organizacyjnej oraz jest stosowana w inżynierii oprogramowania.

Tabela 1. Klasyfikacja zagrożeń dla cyberbezpieczeństwa w lotnictwie cywilnym

Kryterium klasyfikacji	Klasyfikacja i przykłady zagrożeń	Przykłady referencji
Lokalizacja źródła	- zewnętrzne – intencjonalny atak z zewnątrz na systemy informacyjne lotnictwa, np. atak zagłuszający (ang. *Jamming*), - wewnętrzne – zagrożenia umyślne i nieumyślne, np. błąd ludzki, nieuprawnione udostępnienie danych wrażliwych, przekroczenie uprawnień	Cieślak[22] Felski[23]
Przyczyna, źródło	- naturalne – katastrofy naturalne, ekstremalne warunki pogodowe, które mogą powodować np. zakłócenia w telekomunikacji lotniczej, - techniczne – awarie techniczne np. systemów i urządzeń telekomunikacji lotniczej, - działalność człowieka – zagrożenia umyślne i nieumyślne, m.in. fałszowanie sygnału i podszywanie się (ang. *Spoofing*), np. ataki na systemy nawigacji satelitarnej	Bielawski[24] Cieślak[25]
Obiekt ataku	- ataki na systemy kontroli ruchu lotniczego, - ataki na systemy nawigacyjne, - ataki na systemy Internetu Rzeczy itp.	Habler i in.[26]

[18] Zob. L. Zeng, B. Wang, J. Tian, Z. Wang, *Threat impact analysis to air traffic control systems through flight delay modeling*, „Computers & Industrial Engineering" 2021, nr 162, https://doi.org/10.1016/j.cie.2021.107731 [dostęp: 13.04.2023].

[19] Zob. E. Habler, R. Bitton, A. Shabtai, *Evaluating*…, dz. cyt.

[20] Zob. X. Yu, H. Man, X. Jiyu, *Impact of Emerging Network Attack and Defense Technologies on Civil Aviation Information Systems*, 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology, Changsha, 2021, https://doi.org/10.1109/ICCASIT53235.2021.9633537 [dostęp: 13.04.2023], s. 1170–1174.

[21] Zob. M.R. Manesh, N. Kaabouch, *Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system*, „International Journal of Critical Infrastructure Protection" 2017, nr 19, https://doi.org/10.1016/j.ijcip.2017.10.002 [dostęp: 13.04.2023], s. 16–31.

[22] Zob. E. Cieślak, *Bezpieczeństwo cybernetyczne w lotnictwie cywilnym*, „SECRETUM. Służby specjalne, bezpieczeństwo, informacja" 2016, nr 2(5), s. 71–82.

[23] Zob. A. Felski, *Strategie monitorowania zagrożeń systemu EGNOS,* [w:] *Wybrane aspekty zabezpieczenia nawigacji lotniczej*, cz. 2, red. J. Ćwiklak, LAW, Dęblin 2020, s. 67–82.

[24] Zob. R. Bielawski, *Bezpieczeństwo bezzałogowych systemów powietrznych w środowisku zakłóceń*, „O Bezpieczeństwie i Obronności" 2019, nr 2, s. 193–212.

[25] Zob. E. Cieślak, *Bezpieczeństwo...*, dz. cyt.

[26] Zob. E. Habler, R. Bitton, A. Shabtai, *Evaluating the Security of Aircraft Systems*, https://arxiv.org/pdf/2209.04028.pdf [dostęp: 13.04.2023].

 DOI: 10.55676/asi.v3i1.32

Atrybuty bezpieczeństwa informacji	- ataki na poufność – np. atak MITM (ang. *Man in the Middle*) na systemy komunikacji radiowej, - ataki na integralność – np. atak SQL *Injection* w formularzu rezerwacji biletów lotniczych, - ataki na dostępność – np. atak DDoS (ang. *Distributed Denial of Service*) na systemy kontroli ruchu lotniczego; atak *Ransomware* na systemy IT portu lotniczego	Handler[27] Ishtiaq i in.[28] Kumar i in.[29] Zhang i in.[30]
Model STRIDE	- *Spoofing* – podszywanie się, np. *Phishing*; fałszowanie sygnałów GPS, - *Tampering* – manipulacja, modyfikacja, np. sabotaż systemów sterowania lotem; włamania do systemu kontroli lotów w celu modyfikacji parametrów; atak SQL *Injection*, - *Repudiation* – odrzucenie, zaprzeczenie, np. atak typu *Replay* przeprowadzony w celu ukrycia śladów ataku, - *Information disclosure* – ujawnienie informacji, np. atak na systemy rezerwacji biletów, atak XSS (ang. *Cross-Site Scripting*) w celu uzyskania i ujawnienia danych osobowych, - *Denial of Service* – odmowa usługi, np. atak DDoS na serwery w celu uniemożliwienia obsługi ruchu lotniczego, - *Elevation of privileges* – podniesienie uprawnień, np. nieuprawnione uzyskanie dostępu do systemów; atak typu przepełnienie bufora (ang. *buffer overflow*) w celu przejęcia kontroli nad systemem	Alqushayr[31] Tsao i in.[32]
Model TCP/IP (lub model OSI)	- ataki w warstwie aplikacji – np. łamanie haseł; atak słownikowy (ang. *dictionary attack*) na systemy przetwarzania danych pasażerów, - ataki w warstwie transportowej – np. atak MITM, atak DDoS, atak SYN *flood*, - ataki w warstwie Internet – np. IP *Spoofing*, - ataki w warstwie dostępu do sieci – np. GPS *Spoofing*	Siergiejczyk i in.[33] Tsao i in.[34]

Źródło: opracowanie własne.

Odnosząc się do współczesnego środowiska bezpieczeństwa sektora lotniczego, istotnym źródłem informacji są dane dotyczące incydentów bezpieczeństwa. Jako przykład można tu wskazać interaktywną mapę odnotowanych cyberataków[35], która jest opracowana i aktualizowana przez Europejski Zespół Reagowania na Incydenty Komputerowe w Zarządzaniu Ruchem Lotniczym (EATM-CERT), czyli jednostkę

[27] Zob. S. Handler, E. Schroeder, F., Schroeder, T. Herr, *Countering Ransomware: Lesson from Aircraft Hijacking*, https://www.jstor.org/stable/pdf/resrep35077.pdf [dostęp: 14.04.2023].

[28] Zob. S. Ishtiaq, N.A. Abd Rahman, *Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry*, [w:] *International Conference on Integrated Intelligent Computing Communication & Security*, Atlantis Press 2021, https://doi.org/10.2991/ahis.k.210913.071 [dostęp: 13.04.2023], s. 559–567.

[29] Zob. M. Surendra Kumar, G.S. Kasbekar, A. Maity, *Identification of GPS Spoofing as a Drone Cyber--vulnerability and Evaluation of Efficacy of Asynchronous GPS spoofing*, „IFAC-PapersOnLine" 2022, nr 55(22), https://doi.org/10.1016/j.ifacol.2023.03.066 [dostęp: 13.04.2023], s. 394–399.

[30] Zob. R. Zhang, G. Liu, J. Liu, J.P. Nees, *Analysis of Message Attacks in Aviation Data-Link Communication*, „IEEE Access" 2018, nr 6, https://doi.org/10.1109/ACCESS.2017.2767059 [dostęp: 13.04.2023], s. 455–463.

[31] Zob. D.F. Alqushayri, *Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems*, https://commons.erau.edu/cgi/viewcontent.cgi?article=1519&context=edt [dostęp: 17.04.2023].

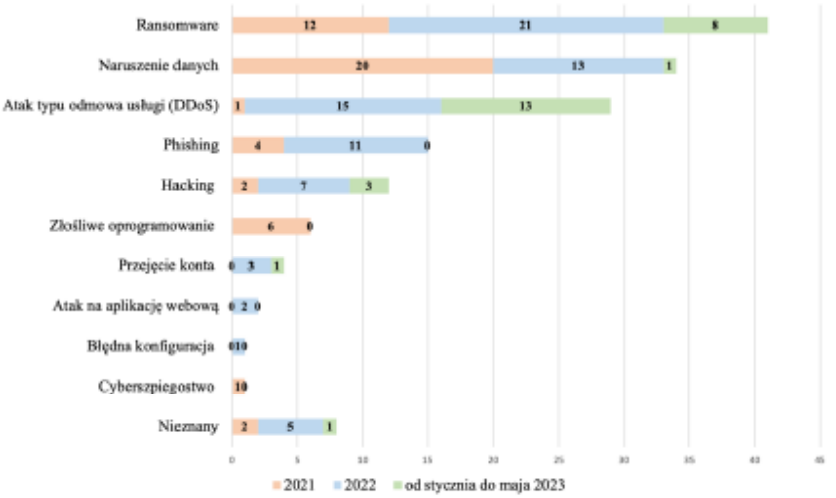
[32] Zob. K.-Y. Tsao, T. Girdler, V.G. Vassilakis, *A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks*, „Ad Hoc Networks" 2022, nr 133, https://doi.org/10.1016/j.adhoc.2022.102894 [dostęp: 13.04.2023].

[33] Zob. M. Siergiejczyk, E. Dudek, *Problematyka bezpieczeństwa informacyjnego w systemach wymiany danych lotniczych*, „Prace Naukowe Politechniki Warszawskiej. Transport" 2017, t. 118, s. 235–246.

[34] Zob. K.-Y. Tsao, T. Girdler, V.G. Vassilakis, *A survey*..., dz. cyt.

[35] EATM-CERT Aviation Cyber Events Map, https://www.google.com/maps/d/embed?mid=1ptVIma0CZqo-PiN-zsomzbRVQDRS7BXGk [dostęp: 6.06.2023].

powołaną przez EUROCONTROL. Na podstawie przeglądu cyberataków zamieszczonych na mapie opracowano rysunek 1, który przedstawia zagregowane dane o cyberatakach w sektorze lotniczym w latach 2021–2022 oraz od stycznia do maja 2023 r.



Rys. 1. Incydenty bezpieczeństwa w sektorze lotniczym
Źródło: opracowanie własne na podstawie: EATM-CERT..., dz. cyt.

Zgodnie z rysunkiem 1 w okresie od stycznia 2021 r. do maja 2023 r. odnotowano łącznie 153 incydenty bezpieczeństwa w sektorze lotniczym. W analizowanym okresie najwięcej zgłoszono ataków: *ransomware* (26,8%), naruszenia danych (22,2%) oraz DDoS (19%). Porównując natomiast dwa pełne lata, w 2022 r. zrealizowano o 175% więcej ataków *ransomware* w stosunku do roku poprzedniego. Atak ten polega na zaszyfrowaniu plików przechowywanych na dysku lokalnym lub w lokalizacji sieciowej oraz na żądaniu wpłacenia środków finansowych w zamian za podanie klucza deszyfrującego. Jako przykład można tu wskazać atak *ransomware* na Agencję ds. Bezpieczeństwa Żeglugi Powietrznej w Afryce i na Madagaskarze (ASECNA)[36]. Kolejny z wymienionych incydentów związany z naruszeniem danych dotyczy nieuprawnionego dostępu do informacji wrażliwych, któremu często towarzyszy ich udostępnienie. Przykładem jest atak na tureckie linie lotnicze Pegasus Airlines, który doprowadził do ujawnienia 23 milionów plików o łącznym rozmiarze 6,5 TB[37]. Ataki DDoS są następnym, istotnym zagrożeniem dla branży lotniczej. Warto przy tym zaznaczyć, że w 2022 r. nastąpił wzrost tych ataków o 1500% w porównaniu do 2021 r. Do przykładowych incydentów można zaliczyć ataki na porty lotnicze w Słowacji i w Bułgarii[38]. Inne istotne rodzaje ataków w latach 2021 – marzec 2023 to *phishing* (9,8%) oraz *hacking* (7,8%). Najmniej incydentów dotyczyło złośliwego oprogramowania (3,9%), przejęcia konta (2,6%),

[36] Tamże.
[37] Tamże.
[38] Tamże.

 DOI: 10.55676/asi.v3i1.32

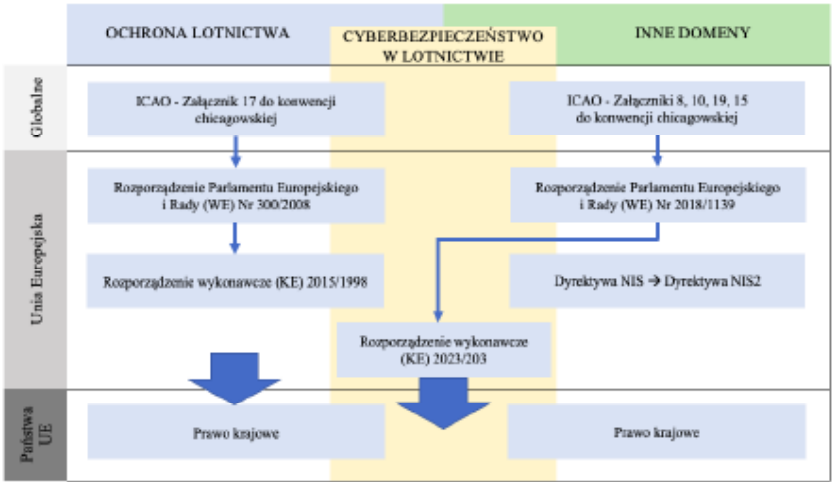
ataków na aplikacje webowe (1,3%), błędnej konfiguracji (0,7%) oraz cyberszpiegostwa (0,7%). Przy czym, około 5,2% ataków zaklasyfikowano jako „nieznany".

Podsumowując rozważania zawarte w niniejszej części artykułu, można stwierdzić, iż w ostatnich latach nasiliły się cyberzagrożenia dla lotnictwa cywilnego. Odnotowane w ostatnim czasie incydenty cyberbezpieczeństwa dotyczyły głównie ataków: *ransomware*, naruszenia danych oraz DDoS. Tego typu działania są motywowane w szczególności względami finansowymi, uzyskaniem dostępu do danych wrażliwych oraz w przypadku niektórych zagrożeń także czynnikami politycznym, religijnym i ideologicznym. Z punktu widzenia bezpieczeństwa narodowego i obronności szczególnie niebezpieczne są także ataki typu APT, których celem jest często działalność cyberszpiegowska lub osłabienie zdolności danego państwa.

4. RAMY PRAWNE CYBERBEZPIECZEŃSTWA W LOTNICTWIE CYWILNYM

W ostatnich latach konieczne stało się podjęcie działań na rzecz cyberbezpieczeństwa w lotnictwie cywilnym, ze względu na rosnące zagrożenia związane z cyberatakami. Skala tych zagrożeń i ich potencjalnych skutków skłoniła interesariuszy lotnictwa cywilnego do wdrożenia inicjatyw mających na celu poprawę cyberbezpieczeństwa w sektorze[39]. Regulacje prawne stanowią istotny element funkcjonowania lotnictwa cywilnego, bowiem mogą określać obowiązki w zakresie wdrożenia konkretnych rozwiązań.

Na rysunku 2 przedstawiono główne akty prawne odnoszące się do cyberbezpieczeństwa w lotnictwie cywilnym z uwzględnieniem perspektywy międzynarodowej, unijnej i krajowej.



Rys. 2. Ramy prawne cyberbezpieczeństwa w lotnictwie cywilnym

Źródło: opracowanie na podstawie: „Strategy for Cybersecurity in Aviation", dz. cyt.

[39] E. Cieślak, *Bezpieczeństwo*..., dz. cyt., s. 8.

Zgodnie z rysunkiem 2 wymagania prawne w zakresie cyberbezpieczeństwa są zawarte zarówno w regulacjach dotyczących ochrony lotnictwa, jak i w aktach prawnych dotyczących innych dziedzin. Odnosząc się do poszczególnych przepisów, w załączniku 17 do Konwencji o międzynarodowym lotnictwie cywilnym (konwencja chicagowska), dodano normę 4.9.1 oraz zalecenie 4.9.2. W normie określono konieczność identyfikacji w dokumentach krajowych krytycznych systemów technologii ICT i danych, które są wykorzystywane w lotnictwie cywilnym, a także opracowanie i wdrożenie środków wynikających z oceny ryzyka oraz zapewniających ochronę tych systemów i danych przed bezprawną ingerencją. Natomiast zalecenie odnosi się do zapewnienia atrybutów bezpieczeństwa informacji i ochrony zidentyfikowanych systemów krytycznych i danych. Jako zalecane środki wskazano np. zapewnienie bezpieczeństwa na etapie projektowania systemu, ochronę łańcucha dostaw, separację sieci, ochronę bądź ograniczenie możliwości zdalnego dostępu[40]. Ponadto w europejskiej Strategii Cyberbezpieczeństwa w Lotnictwie zaznaczono, iż kompleksowe podejście do omawianej problematyki może wymagać uwzględnienia postanowień dotyczących poufności, integralności i dostępności, także w innych załącznikach do konwencji chicagowskiej, tj. 8, 10, 19 i 15[41].

Do innych dokumentów ICAO można zaliczyć Strategię Cyberbezpieczeństwa Lotnictwa, która określa filary cyberbezpieczeństwa, tj.: współpraca międzynarodowa, zarządzanie, ustawodawstwo i regulacje, polityka cyberbezpieczeństwa, udostępnianie informacji, zarządzanie incydentami i planowanie awaryjne oraz budowanie potencjału, szkolenia i kultura cyberbezpieczeństwa[42]. Założenia określone w Strategii zostały doprecyzowane w Planie działań w zakresie cyberbezpieczeństwa. W dokumencie tym dla każdego z filarów wymienionych w Strategii przyjęto 32 działania, które zostały podzielone na 51 zadań zalecanych do realizacji[43]. Problematyka cyberbezpieczeństwa została podkreślona także w rezolucjach Zgromadzenia ICAO. Najnowszym dokumentem w omawianym zakresie jest rezolucja A41-19 z 2022 r., która określa zestaw działań w zakresie przeciwdziałania zagrożeniom cybernetycznym dla lotnictwa cywilnego[44].

Przechodząc do regulacji unijnych, kluczowym dokumentem jest Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008, które jako jeden z głównych celów wskazało opracowanie podstaw do interpretacji załącznika 17 do konwencji chicagowskiej w odniesieniu do normy i zalecenia w zakresie cyberbezpieczeństwa[45]. Kolejnym dokumentem jest Rozporządzenie wykonawcze Komisji (UE) 2015/1998 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych norm

40 Załącznik 17 do Konwencji o międzynarodowym lotnictwie cywilnym, „Ochrona międzynarodowego lotnictwa cywilnego przed Aktami Bezprawnej Ingerencji", ICAO, marzec 2020.

41 „Strategy for Cybersecurity in Aviation", dz. cyt.

42 „Aviation Cybersecurity Strategy…", dz. cyt.

43 Zob. „Cybersecurity Action Plan", dz. cyt.

44 Resolution A41-19: Addressing Cybersecurity in Civil Aviation, ICAO, https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf [dostęp: 24.04.2023].

45 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (OJ L 97, 9.4.2008).

 DOI: 10.55676/asi.v3i1.32

ochrony lotnictwa cywilnego[46]. Rozporządzenie to było kilkukrotnie nowelizowane, przy czym istotne środki bezpieczeństwa cybernetycznego wprowadziło Rozporządzenie wykonawcze Komisji (UE) 2019/1583[47]. W regulacji jednym z podstawowych założeń jest identyfikacja systemów technologii ICT i danych krytycznych oraz ich ochrona przed cyberzagrożeniami. Inną istotną regulacją jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139, które określa wspólne zasady lotnictwa cywilnego oraz doprecyzowuje zadania Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA). W rozporządzeniu podkreślono m.in. konieczność współpracy oraz stosowania środków uwzględniających zależności między różnymi obszarami bezpieczeństwa lotniczego oraz bezpieczeństwem lotniczym, cyberbezpieczeństwem, a także innymi technicznymi obszarami uregulowań dotyczących lotnictwa[48]. Zasady zarządzania ryzykiem w bezpieczeństwie informacji zdefiniowano w Rozporządzeniu wykonawczym Komisji (UE) 2023/203. Regulacja wprowadza wymagania dotyczące systemu zarządzania bezpieczeństwem informacji, oceny ryzyka, postępowania z ryzykiem, zarządzania incydentami bezpieczeństwa oraz podkreśla potrzebę ciągłego doskonalenia[49].

Kontynuując charakterystykę regulacji unijnych, kluczowe znaczenie ma także tzw. Dyrektywa NIS[50] i jej zrewidowana wersja tzw. Dyrektywa NIS2[51]. Dokumenty te zobowiązały państwa członkowskie do wdrożenia rozwiązań w dziedzinie cyberbezpieczeństwa, w tym także w lotnictwie cywilnym. Wśród istotnych założeń jest

[46] Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 lipca 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (OJ L 299.1, 14.11.2015).

[47] Rozporządzenie wykonawcze Komisji (UE) 2019/1583 z dnia 25 września 2019 r. zmieniające rozporządzenie wykonawcze (UE) 2015/1998 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego w odniesieniu do środków w zakresie cyberbezpieczeństwa (OJ L 246, 26.9.2019).

[48] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (PE/2/2018/REV/1).

[49] Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w kwestii wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373 i (UE) 2021/664 oraz właściwych organów objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012, (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373, (UE) nr 139/2014 i (UE) 2021/664 oraz zmieniające rozporządzenia Komisji (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664 (OJ L 31, 2.2.2023).

[50] Zob. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (OJ L 191/1, 19.7.2016).

[51] Zob. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (OJ L 333, 27.12.2022).

obowiązek wdrożenia krajowych regulacji zapewniających zgodność z przepisami unijnymi, w tym odnoszących się m.in. do kwestii zarządzania ryzykiem, zarządzania incydentami i zarządzania ciągłością działania[52].

Przechodząc do ostatniego poziomu regulacji wyszczególnionych na rysunku 2, obejmuje on prawo krajowe uchwalone w poszczególnych państwach. Jako przykład można tu wskazać ustawę o krajowym systemie cyberbezpieczeństwa, która implementuje do krajowego systemu prawnego przywołaną wcześniej dyrektywę NIS. W związku z tym, że jest to pierwszy akt prawny rangi ustawowej regulujący kompleksowo kwestie cyberbezpieczeństwa, zostanie on szerzej omówiony w następnej części artykułu.

Wymienione w publikacji regulacje dowodzą złożoności systemu prawnego dotyczącego cyberbezpieczeństwa w lotnictwie cywilnym. Warto przy tym zaznaczyć, że nie wyczerpują one w całości omawianego zagadnienia, ale określają ogólne ramy prawne. Wśród innych wartych uwagi można wskazać m.in. reguły EASA, np. RMT.0648, odnosząca się do cyberbezpieczeństwa statków powietrznych[53], bądź RMT.0720, wprowadzająca zasady zarządzania ryzykiem[54]. Istotne są także normy, standardy i inne dokumenty związane z przemysłem lotniczym. Wartymi uwagi są np. dokumenty Europejskiej Organizacji ds. Bezpieczeństwa Żeglugi Powietrznej (EUROCONTROL)[55], Międzynarodowego Zrzeszenia Przewoźników Powietrznych (IATA)[56] czy Organizacji Służb Cywilnej Żeglugi Powietrznej (CANSO)[57]. W praktyce wdrażania rozwiązań w zakresie cyberbezpieczeństwa stosowane są także normy i standardy opracowane przez organizacje niezwiązane z branżą lotniczą, np. przez Międzynarodową Organizację Normalizacyjną (ISO) bądź Narodowy Instytut Standaryzacji i Technologii (NIST).

5. LOTNICTWO CYWILNE JAKO ELEMENT KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA RP

Dyrektywa NIS jest regulacją unijną, która w istotnym stopniu wpłynęła na funkcjonowanie krajowych rozwiązań w zakresie cyberbezpieczeństwa. W dyrektywie wskazano sektory objęte jej przepisami, wśród których jest m.in. transport lotniczy. Jak już wspomniano w poprzedniej sekcji, aktem prawnym implementującym w Polsce unijny dokument jest ustawa o krajowym systemie cyberbezpieczeństwa. Ustawa była kilkukrotnie nowelizowana, przy czym w przyszłości można spodziewać się

[52] D. Markopoulou, V. Papakonstantinou, P. Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, „Computer Law & Security Review" 2019, nr 35(6), https://doi.org/10.1016/j.clsr.2019.06.007 [dostęp: 27.04.2023].

[53] Zob. „Aircraft cybersecurity", RMT.0648, Issue 1, EASA, 2016, https://www.easa.europa.eu/en/document-library/terms-of-reference-and-group-compositions/tor-rmt0648 [dostęp: 27.04.2023].

[54] Zob. „Cybersecurity risks", RMT.0720, Issue 1, EASA, https://www.easa.europa.eu/en/document-library/terms-of-reference-and-group-compositions/tor-rmt0720 [dostęp: 27.04.2023].

[55] Zob. np. „ATM Cybersecurity Maturity Model Level 1", EUROCONTROL, 2017, https://www.eurocontrol.int/publication/atm-cybersecurity-maturity-model [dostęp: 27.04.2023].

[56] Zob. np. „IOSA Standards Manual (ISM)", Edition 16, IATA, 2023.

[57] Zob. np. „CANSO Standard of Excellence in Cybersecurity", CANSO, 2020.

 DOI: 10.55676/asi.v3i1.32

następnej nowelizacji z uwagi na konieczność zapewnienia zgodności z Dyrektywą NIS2. Niemniej, ustawa w aktualnym kształcie jest wciąż obowiązująca, a jej nowelizacja powinna nastąpić najpóźniej w październiku 2024 r.

Analizując problematykę lotnictwa cywilnego w kontekście krajowego systemu cyberbezpieczeństwa, warto zaznaczyć, że system ten ma złożoną strukturę, która obejmuje np. organy właściwe ds. cyberbezpieczeństwa, operatorów usług kluczowych, dostawców usług cyfrowych, Zespoły Reagowania na incydenty bezpieczeństwa komputerowego, instytuty badawcze, Polską Agencję Żeglugi Powietrznej[58]. Głównym celem systemu jest:

> zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[59].

W kontekście powyższych rozważań i lotnictwa cywilnego istotne znaczenie ma pojęcie usługi kluczowej, które oznacza usługę mającą „kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych”[60]. W rozporządzeniu wydanym na podstawie delegacji ustawowej i stanowiącym wykaz usług kluczowych wymieniono następujące ich rodzaje w transporcie lotniczym: transport lotniczy pasażerski, transport lotniczy towarów oraz działalność usługowa wspomagająca transport lotniczy realizowana przez: zarządzającego lotniskiem, przedsiębiorcę posiadającego status zarejestrowanego agenta, przedsiębiorcę posiadającego status agenta obsługi naziemnej bądź instytucję zapewniającą służby żeglugi powietrznej[61].

Podmiotem odpowiedzialnym za cyberbezpieczeństwo wymienionych wyżej usług jest operator usługi kluczowej. Identyfikacja operatorów następuje w wyniku decyzji administracyjnej wydanej przez organ właściwy ds. cyberbezpieczeństwa. W przypadku transportu lotniczego organem uprawnionym jest minister właściwy ds. transportu, czyli aktualnie Minister Infrastruktury. Za operatora usługi kluczowej może być uznany: przewoźnik lotniczy, zarządzający lotniskiem, przedsiębiorca bądź instytucja zapewniająca służby żeglugi powietrznej. Operator posiada obowiązki wynikające z ustawy, które realizuje w terminie 3, 6 lub 12 miesięcy od dnia doręczania decyzji administracyjnej (tabela 2).

[58] Dz.U. z 2018 r., poz. 1560.
[59] Tamże.
[60] Tamże.
[61] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018 r., poz. 1806).

Tabela 2. Obowiązki operatora usługi kluczowej

Termin	Obowiązki
3 miesiące	- systematyczne szacowanie ryzyka oraz zarządzanie tym ryzykiem, - zarządzanie incydentami, - wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami KSC, - zapewnienie dostępu do wiedzy, - zgłaszanie incydentów poważnych, - powołanie struktur wewnętrznych lub zawarcie umowy z podmiotem zewnętrznym w celu świadczenia usług cyberbezpieczeństwa
6 miesięcy	- wdrożenie zabezpieczeń organizacyjnych i technicznych, które są adekwatne do oszacowanego ryzyka oraz uwzględniają aktualny stan wiedzy, - gromadzenie informacji o zagrożeniach i podatnościach, - implementacja działań zapobiegawczych i ograniczających skutki incydentów, - stosowanie środków łączności, które zapewniają bezpieczną i niezakłóconą komunikację, - przygotowanie, wdrożenie i aktualizacja dokumentacji cyberbezpieczeństwa (dokumentacja normatywna i operacyjna)
12 miesięcy	- przygotowanie pierwszego audytu bezpieczeństwa (kolejne realizowane są co najmniej raz na 2 lata), - przekazanie sprawozdania z audytu na wniosek organu właściwego ds. cyberbezpieczeństwa, dyrektora RCB, Szefa ABW

Źródło: opracowanie własne na podstawie: Dz.U. z 2018 r., poz. 1560.

Zgodnie z tabelą 2 podmioty sektora lotniczego uznane za operatora usługi kluczowej są zobowiązane do realizacji określonych zadań w zakresie cyberbezpieczeństwa. Istotnym obowiązkiem jest wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) obejmującego system, który jest wykorzystywany do świadczenia usługi kluczowej. Do innych należą np.: zarządzanie ryzykiem, wdrożenie zabezpieczeń, zarządzanie incydentami, audyt bezpieczeństwa, ustanowienie struktur organizacyjnych, opracowanie dokumentacji normatywnej i operacyjnej oraz zapewnienie dostępu do wiedzy.

W realizacji wymienionych obowiązków pomocne są normy i standardy. Przykładowo w rozporządzeniu odnoszącym się do dokumentacji normatywnej i operacyjnej[62] wskazano, iż dokumentacja SZBI powinna być wytworzona zgodnie z wymaganiami zawartymi w normie ISO/IEC 27001[63], natomiast dokumentacja dotycząca zarządzania ciągłością działania w oparciu o normę ISO 22301[64]. Warto także zwrócić uwagę na zbiór polskich standardów opublikowanych jako Narodowe Standardy Cyberbezpieczeństwa (NSC). Dokumenty te zostały opracowane na podstawie amerykańskich standardów NIST i są rekomendowane do stosowania przez podmioty krajowego systemu cyberbezpieczeństwa RP. NSC obejmują zagadnienia dotyczące np.: zarządzania

[62] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r., poz. 2080).

[63] Zob. PN-EN ISO 27001:2017-06, dz. cyt.

[64] Zob. PN-EN ISO 22301:2020-04, „Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania", PKN, Warszawa 2021.

 DOI: 10.55676/asi.v3i1.32

ryzykiem[65], wdrożenia zabezpieczeń[66], postępowania z incydentami bezpieczeństwa[67], planowania awaryjnego[68] i bezpieczeństwa systemów sterownia przemysłowego[69].

Podsumowując, unijna dyrektywa NIS i implementująca ją ustawa o krajowym systemie cyberbezpieczeństwa stanowią ważne przedsięwzięcie w kierunku zapewnienia cyberbezpieczeństwa w lotnictwie cywilnym. Implementacja przyjętych wymagań może przyczynić się do ochrony przed cyberatakami i zminimalizowania ryzyka zakłóceń w transporcie lotniczym. Jednocześnie, podmioty sektora staną w przyszłości w obliczu wyzwań związanych z dostosowaniem wewnętrznych rozwiązań do nowych regulacji prawnych, czyli dyrektywy NIS2, oraz, jak można przypuszczać, znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa.

6. WNIOSKI

W artykule przedstawiono terminologię, klasyfikację zagrożeń oraz ramy prawne cyberbezpieczeństwa w lotnictwie cywilnym. Ponadto odniesiono się do krajowego systemu cyberbezpieczeństwa RP z uwzględnieniem charakterystyki operatorów usług kluczowych w sektorze lotniczym. Przegląd literatury przedmiotu dowodzi, że problematyka ochrony przed cyberzagrożeniami stanowi istotne wyzwanie dla sektora lotniczego. W kontekście powyższych rozważań sformułowano następujące wnioski i rekomendacje:

1. Zapewnienie cyberbezpieczeństwa w lotnictwie cywilnym wymaga perspektywy systemowej i uwzględnienia aspektów prawnych, proceduralno-organizacyjnych, technicznych, fizycznych oraz związanych z czynnikiem ludzkim. Zasadne jest więc przyjęcie kompleksowego podejścia do problematyki cyberbezpieczeństwa w lotnictwie cywilnym, które uwzględni obszar bezpieczeństwa (ang. *safety*) i ochrony (ang. *security*). Specyfika złożoności sektora uzasadnia także potrzebę współpracy i koordynacji między państwami, organizacjami i innymi podmiotami powiązanymi z sektorem lotnictwa.
2. Zagrożenia dla cyberbezpieczeństwa w lotnictwie cywilnym obejmują szerokie spektrum zjawisk mogących prowadzić do incydentów bezpieczeństwa. W artykule zaproponowano klasyfikację, która może być rozwijana zarówno w obszarze eksponowanych zagrożeń, jak i dodatkowych kryteriów podziału. Warto przy tym zaznaczyć, że identyfikacja zagrożeń jest wykorzystywana np. na potrzeby zarządzania ryzykiem, analizy podatności, inżynierii bezpieczeństwa bądź projektowania

[65] NSC 800-39, „Zarządzanie ryzykiem bezpieczeństwa informacji (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2022.

[66] NSC 800-53, „Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (wer.2.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

[67] NSC 800-61, „Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

[68] NSC 800-34, „Poradnik Planowania Awaryjnego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

[69] NSC 800-82, „Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2022.

i implementacji zabezpieczeń. Innymi słowy, zakres analizy zagrożeń jest determinowany w szczególności przyjętym celem oraz specyfiką organizacji.

3. Przegląd odnotowanych w ostatnim czasie incydentów bezpieczeństwa wskazuje na tendencje rozwojowe cyberzagrożeń. Jednocześnie automatyzacja i cyfryzacja rozwiązań o krytycznym znaczeniu dla lotnictwa cywilnego prowadzi do wzrostu ilości potencjalnych obiektów cyberataków. Mając na uwadze aktualne kierunki transformacji cyfrowej, niezbędne jest monitorowanie i doskonalenie istniejących rozwiązań. Kluczowe są także inwestycje na badania i rozwój w dziedzinie cyberbezpieczeństwa lotnictwa cywilnego. Rekomendowana jest więc współpraca przemysłu lotniczego, uczelni wyższych i instytutów badawczych w obszarze nowych technologii, metod i praktyk zwiększających skuteczność ochrony przed cyberatakami. Potencjał wykazują takie rozwiązania jak np. Blockchain, sztuczna inteligencja i uczenie maszynowe, dlatego też zasadne jest kontynuowanie badań nad ich rozwojem na potrzeby cyberbezpieczeństwa w lotnictwie cywilnym.
4. Przegląd regulacji prawnych dotyczących cyberbezpieczeństwa w lotnictwie cywilnym pozwala przyjąć ogólny ich podział na przepisy międzynarodowe, regionalne i krajowe. Kluczową rolę odgrywają także normy i standardy, w tym także rozwiązania branżowe. Biorąc pod uwagę ich różnorodność, problematyczne wydaje się opracowanie dokumentów wewnętrznych, które zapewnią zgodność z wszystkimi wymaganiami prawnymi. Na problem ten zwrócono uwagę w raporcie Ministerstwa Infrastruktury, w którym operatorzy usług kluczowych z branży lotniczej jako wyzwanie wskazali zapewnienie zgodności z ustawą o krajowym systemie cyberbezpieczeństwa, w powiązaniu z przepisami z innych obszarów[70]. Odnosząc się do zasygnalizowanych problemów, uzasadnione jest zatem dążenie do harmonizacji przepisów.
5. Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła obowiązki na wiele podmiotów sektora lotniczego. Wśród istotnych należy wskazać operatorów usług kluczowych, którzy zostali zobowiązani do wdrożenia odpowiedniej dokumentacji, zabezpieczeń i rozwiązań organizacyjnych. Wyniki badań opublikowane w raporcie Ministerstwa Infrastruktury wykazały, że operatorzy usług kluczowych do głównych wyzwań zaliczyli: ograniczenia finansowe, szkolenia, budowanie świadomości, problemy z pozyskaniem personelu, wyzwania technologiczne i organizacyjne, pogodzenie potrzeb biznesowych i cyberbezpieczeństwa[71]. Mając na uwadze wymienione wyżej problemy, zasadne jest podjęcie badań naukowych uwzględniających przyszłe wyzwania związane z wdrożeniem Dyrektywy NIS2 w sektorze.

[70] „Dojrzałość w obszarze cyberbezpieczeństwa w sektorze transportu w Polsce. Raport 2022", Ministerstwo Infrastruktury, s. 43.

[71] Tamże, s. 42.

 DOI: 10.55676/asi.v3i1.32

BIBLIOGRAFIA

Artykuły i monografie

Bielawski R., *Bezpieczeństwo bezzałogowych systemów powietrznych w środowisku zakłóceń*, „O Bezpieczeństwie i Obronności" 2019, nr 2.

Cieślak E., *Bezpieczeństwo cybernetyczne w lotnictwie cywilnym*, „SECRETUM. Służby specjalne, bezpieczeństwo, informacja" 2016, wyd. 2.

Elmarady A.A., Rahouma K., *Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment*, „IEEE Access" 2021, nr 9, https://doi.org/10.1109/ACCESS.2021.3121230.

Felski A., *Strategie monitorowania zagrożeń systemu EGNOS*, [w:] *Wybrane aspekty zabezpieczenia nawigacji lotniczej*, cz. 2, red. J. Ćwiklak, LAW, Dęblin 2020.

Ishtiaq S., Abd Rahman N.A., *Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry*, [w:] *International Conference on Integrated Intelligent Computing Communication & Security*, Atlantis Press, 2021, https://doi.org/10.2991/ahis.k.210913.071.

Khatun M., Wagner F., Jung R., Glaß M., *Identification of Interface related Factors between Safety Management System and Cybersecurity Management System for Highly Automated Driving Vehicles*, [w:] *Proceedings of the 25th International Conference on Enterprise Information Systems*, red. J. Filipe, M. Śmiałek, A. Brodsky, S. Hammoudi, SciTePress, Prague 2023.

Koroniotis N., Moustafa N., Schiliro F., Gauravaram P., Janicke H., *A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports*, „IEEE Access"2020, nr 8, https://doi.org/10.1109/ACCESS.2020.3036728.

Markopoulou D., Papakonstantinou V., Hert P., *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, „Computer Law & Security Review" 2019, nr 35(6), https://doi.org/10.1016/j.clsr.2019.06.007.

Siergiejczyk M., Dudek E., *Problematyka bezpieczeństwa informacyjnego w systemach wymiany danych lotniczych*, „Prace Naukowe Politechniki Warszawskiej. Transport" 2017, t. 118.

Surendra Kumar M., Kasbekar G., Maity A., *Identification of GPS Spoofing as a Drone Cyber-vulnerability and Evaluation of Efficacy of Asynchronous GPS spoofing*, „IFAC-PapersOnLine" 2022, nr 55(22), https://doi.org/10.1016/j.ifacol.2023.03.066.

Szczepaniuk E., Szczepaniuk H., *Analysis of cybersecurity competencies: Recommendations for telecommunications policy*, „Telecommunications Policy" 2022, nr 46(3), https://doi.org/10.1016/j.telpol.2021.102282.

Szczepaniuk H., Szczepaniuk E., *Cybersecurity Management within the Internet of Things*, [w:] *IoT Security Paradigms and Applications Research and Practices*, red. S.K. Sharma, B. Bhushan, N.C. Debnath, Taylor & Francis Group, Boca Raton 2021.

Thums J., Künzel L., Klumpp M., Bardmann M., Ruiner C., *Future air transportation and digital work at airports – Review and developments*, „Transportation Research Interdisciplinary Perspectives" 2023, nr 19, https://doi.org/10.1016/j.trip.2023.100808.

Tsao K.-Y., Girdler T., Vassilakis V.G., *A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks*, „Ad Hoc Networks"2022, nr 133, https://doi.org/10.1016/j.adhoc.2022.102894.

Yu X., Man H., Jiyu X., *Impact of Emerging Network Attack and Defense Technologies on Civil Aviation Information Systems*, 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology, Changsha, 2021, https://doi.org/10.1109/ICCASIT53235.2021.9633537.

Zeng L., Wang B., Tian J., Wang Z., *Threat impact analysis to air traffic control systems through flight delay modeling*, „Computers & Industrial Engineering" 2021, nr 162, https://doi.org/10.1016/j.cie.2021.10773.

Zhang R., Liu G., Liu J., Nees P.J., *Analysis of Message Attacks in Aviation Data-Link Communication*, „IEEE Access" 2018, nr 6, https://doi.org/10.1109/ACCESS.2017.2767059.

Żmigrodzka M., *Cybersecurity – One of the Greatest Challenges for Civil Aviation in the 21st Century*, „Safety & Defense" 2020, nr 6(2), https://doi.org/10.37105/sd.73.

Akty prawne, normy, standardy i dokumenty strategiczne

„Aviation Cybersecurity Strategy", ICAO, October 2019.

„CANSO Standard of Excellence in Cybersecurity", CANSO, 2020.

„Cybersecurity Action Plan", ICAO, January 2022.

„Dojrzałość w obszarze cyberbezpieczeństwa w sektorze transportu w Polsce. Raport 2022", Ministerstwo Infrastruktury.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (O.J. EU L 191/1, 19.7.2016).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (OJ L 333, 27.12.2022).

„IOSA Standards Manual (ISM)", Edition 16, IATA, 2023.

„Krajowy Program Bezpieczeństwa w Lotnictwie Cywilnym", Ministerstwo Infrastruktury, Urząd Lotnictwa Cywilnego, Warszawa 2020.

NSC 800-34, „Poradnik Planowania Awaryjnego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

NSC 800-39, „Zarządzanie ryzykiem bezpieczeństwa informacji (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2022.

NSC 800-53, „Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (wer.2.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

 DOI: 10.55676/asi.v3i1.32

NSC 800-61, „Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2021.

NSC 800-82, „Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego (wer.1.0)", Pełnomocnik Rządu ds. cyberbezpieczeństwa, Warszawa 2022.

PN-EN ISO 22301:2020-04, „Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania", PKN, Warszawa 2021.

PN-EN ISO 27001:2017-06, „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania", PKN, Warszawa 2017.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (PE/2/2018/REV/1).

Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (OJ L 97, 9.4.2008).

Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018 r., poz. 1806).

Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r., poz. 2080).

Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (OJ L 299.1, 2015).

Rozporządzenie Wykonawcze Komisji (UE) 2019/1583 z dnia 25 września 2019 r. zmieniające rozporządzenie wykonawcze (UE) 2015/1998 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego w odniesieniu do środków w zakresie cyberbezpieczeństwa (OJ L 246, 26.9.2019).

Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w kwestii wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373 i (UE) 2021/664 oraz właściwych

organów objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012, (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373, (UE) nr 139/2014 i (UE) 2021/664 oraz zmieniające rozporządzenia Komisji (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664 (OJ L 31, 2.2.2023).

„Strategy for Cybersecurity in Aviation", First Issue, ESCP, September 2019.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

Załącznik 17 do Konwencji o międzynarodowym lotnictwie cywilnym, „Ochrona międzynarodowego lotnictwa cywilnego przed Aktami Bezprawnej Ingerencji", ICAO, marzec 2020.

Źródła internetowe

Aircraft cybersecurity, RMT.0648, Issue 1, EASA, 2016, https://www.easa.europa.eu/en/document-library/terms-of-reference-and-group-compositions/tor-rmt0648.

Alqushayri D.F., *Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems*, https://commons.erau.edu/cgi/viewcontent.cgi?article=1519&context=edt.

ATM Cybersecurity Maturity Model Level 1, EUROCONTROL, 2017, https://www.eurocontrol.int/publication/atm-cybersecurity-maturity-model.

Cybersecurity Culture in Civil Aviation, ICAO, January 2022, https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf.

Cybersecurity risks, Issue 1, RMT.0720, EASA, https://www.easa.europa.eu/en/document-library/terms-of-reference-and-group-compositions/tor-rmt0720.

HablerE. , BittonR. , Shabtai A., *Evaluating the Security of Aircraft Systems*, https://arxiv.org/pdf/2209.04028.pdf.

EATM-CERT Aviation Cyber Events Map, https://www.google.com/maps/d/embed?mid=1ptVIma0CZqoPiN-zsomzbRVQDRS7BXGk.

ENISA Transport Threat Landscape, European Union Agency for Cybersecurity, 2023, https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.

Handler S., Schroeder E., Schroeder F., Herr T., *Countering Ransomware: Lesson from Aircraft Hijacking*, https://www.jstor.org/stable/pdf/resrep35077.pdf.

Resolution A41-19: Addressing Cybersecurity in Civil Aviation, ICAO, https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf.

Think Paper #12: Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?, EUROCONTROL EATM-CERT Services, 2021, https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper--12-aviation-under-cyber-attack.pdf.

 DOI: 10.55676/asi.v3i1.32