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

KIERUNKI BADAŃ NAD CYBERBEZPIECZEŃSTWEM W LOTNICTWIE CYWILNYM – PRZEGLĄD LITERATURY

https://doi.org/10.55676/asi.v7i1.105

Streszczenie

Celem artykułu jest identyfikacja i charakterystyka głównych kierunków badań nad cyberbezpieczeństwem w lotnictwie cywilnym w latach 2015–2025 (stan na lipiec 2025 r.). Badania oparto o publikacje dostępne w bazie Scopus. Analiza bibliometryczna umożliwiła wskazanie klastrów badawczych, które następnie scharakteryzowano na podstawie literatury. Wyniki określają główne obszary badawcze, takie jak: standaryzacja systemów, zarządzanie ryzykiem, detekcja zagrożeń, wykrywanie anomalii i nowe technologie (np. Internet Rzeczy, Big Data, sztuczna inteligencja, Blockchain). Rzadziej podejmowanym zagadnieniem jest np. wpływ czynnika ludzkiego na cyberbezpieczeństwo w lotnictwie cywilnym. Stwierdzono również niewielką liczbę publikacji przeglądowych, które systematyzują istniejącą wiedzę. Artykuł podkreśla potrzebę holistycznego podejścia do cyberbezpieczeństwa w sektorze lotniczym. Dalsze badania warto koncentrować na integracji nowych technologii, w tym interoperacyjności, standaryzacji i zgodności z regulacjami. Istotne są również kwestie dotyczące czynnika ludzkiego, analizy ryzyka oraz odporności na cyberzagrożenia.

***Słowa kluczowe**: cyberbezpieczeństwo, lotnictwo cywilne, nowe technologie, przegląd literatury, analiza bibliometryczna*

RESEARCH DIRECTIONS ON CYBERSECURITY IN CIVIL AVIATION – LITERATURE REVIEW

Abstract

The article aims to identify and characterize the main directions of research on cybersecurity in civil aviation from 2015 to 2025 (as of July 2025). The research was based on publications available in the Scopus database. Bibliometric analysis enabled the identification of research clusters, which were then characterized based on the literature. The results define key research areas such as system standardization, risk management, threat detection, anomaly detection, and emerging technologies (e.g., Internet of Things, Big Data, Artificial Intelligence, Blockchain). A less frequently discussed issue is, for example, the impact of the human factor on cybersecurity in civil aviation. A limited number of review publications systematizing existing knowledge were also identified. The article emphasizes the need for a holistic approach to cybersecurity in the aviation sector. Further research should focus on the integration of emerging technologies, including interoperability, standardization, and regulatory compliance. Issues related to the human factor, risk analysis, and resilience to cyber threats are also of key importance.

***Keywords**: cybersecurity, civil aviation, emerging technologies, literature review, bibliometric analysis*

1. Wstęp

W ostatnich latach lotnictwo cywilne przechodzi transformację, której podstawą jest rozwój nowoczesnych technologii obejmujący m.in. cyfryzację, automatyzację oraz integrację systemów wspierających kluczowe procesy. Zmiany te są ukierunkowane na zwiększenie bezpieczeństwa i efektywności, a ich zakres dotyczy np. modernizacji systemów zarządzania ruchem lotniczym, operacji naziemnych i systemów obsługi pasażerów. Do przykładowych rozwiązań można zaliczyć systemy ADS-B, zdalne wieże kontroli lotów oraz elektroniczne platformy rezerwacyjne. Wymienione elementy generują wiele korzyści dla funkcjonowania lotnictwa cywilnego, ale stwarzają także nowe wyzwania w obszarze cyberbezpieczeństwa.

Jednym z głównych problemów dotyczących omawianej problematyki jest wzrost ilości cyberataków na transport lotniczy. Tendencja ta znajduje potwierdzenie w danych udostępnionych przez Europejski Zespół Reagowania na Incydenty Komputerowe w Zarządzaniu Ruchem Lotniczym (EATM-CERT)[1]. Podkreślić należy, że cyberzagrożenia mają wielowymiarowe konsekwencje oraz odnoszą się do

[1] Zob. https://www.google.com/maps/d/embed?mid=1ptVIma0CZqoPiN-zsomzbRVQDRS7BXGk [dostęp: 30.06.2025].

różnych obszarów działalności sektora lotniczego. Cyberataki skutkują m.in. zakłóceniami w zarządzaniu ruchem lotniczym, naruszeniem integralności systemów oraz nieuprawnionym dostępem do danych osobowych. Mogą one mieć również wymiar prawny i ekonomiczny, który prowadzi do strat finansowych, a także szkód wizerunkowych i utraty zaufania pasażerów.

Z zarysowanego kontekstu wynika, że cyberbezpieczeństwo jest istotnym wyzwaniem dla lotnictwa cywilnego. Znaczenie tego zagadnienia zostało również podkreślone w dokumentach opracowanych przez organizacje zajmujące się bezpieczeństwem w tym sektorze. Jako przykład można wskazać Globalny Plan Ochrony Lotnictwa Cywilnego, który opracowała Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO)[2]. Dokument wymienia sześć głównych obszarów priorytetowych, w tym także związanych z ochroną cyberprzestrzeni. Plan podkreśla potrzebę integracji cyberbezpieczeństwa z procesami wdrażania technologii w celu zapobiegania powstaniu nowych podatności w systemie ochrony lotnictwa cywilnego[3]. Ponadto zwraca on uwagę na zarządzanie ryzykiem, cyberhigienę i rolę czynnika ludzkiego.

Na podstawie przeglądu literatury przedmiotu można zaobserwować intensyfikację badań nad cyberbezpieczeństwem w lotnictwie cywilnym. Wyrazem tego jest rosnąca liczba publikacji naukowych poświęconych omawianemu zagadnieniu. Początkowe prace koncentrowały się głównie na ogólnych aspektach ochrony infrastruktury krytycznej, a problematyka cyberbezpieczeństwa w lotnictwie była postrzegana jako element szerszego kontekstu[4]. Inne prace dotyczyły m.in. bezpieczeństwa informacji[5], zabezpieczenia sieci komputerowej[6], zagrożeń[7] czy też przyszłości lotnictwa cywilnego[8]. Dalszy rozwój badań naukowych przyczynił się do systematycznego wzrostu ilości publikacji, co wskazuje na rosnące znaczenie bezpieczeństwa cyberprzestrzeni w sektorze lotniczym. Niemniej jednak wśród dostępnych opracowań istnieje niewiele artykułów przeglądowych, które porządkują wiedzę w tej dziedzinie.

Mając na uwadze istniejącą lukę badawczą, celem niniejszego artykułu jest identyfikacja oraz charakterystyka głównych kierunków badań nad cyberbezpieczeństwem w lotnictwie cywilnym. Na potrzeby realizacji przyjętego celu przeglądowi poddano literaturę naukową, którą opublikowano w okresie od stycznia 2015 r. do lipca 2025 r. Natomiast główny problem badawczy sformułowano w postaci następującego pytania: Jakie są dominujące kierunki badań nad cyberbezpieczeństwem w lotnictwie cywilnym w analizowanym okresie?

Obserwacje oparto na analizie bibliometrycznej danych pozyskanych z bazy Scopus. Do opracowania wyników wykorzystano oprogramowanie Microsoft Excel oraz VOSviewer. Istotnym elementem była analiza współwystępowania słów kluczowych. Umożliwiła ona wyodrębnienie klastrów badawczych, które następnie scharakteryzowano na podstawie literatury przedmiotu.

[2] Zob. https://www.icao.int/icao-global-aviation-security-plan-gasep [dostęp: 30.06.2025].
[3] Global Aviation Security Plan (GASeP), Doc 10118, ICAO 2024.
[4] Zob. S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies*, „IEEE Control Systems Magazine" 2001, t. 21, nr 6, s. 11–25, https://doi.org/10.1109/37.969131.
[5] Zob. H. Chang i in., *The Case Study of Information Security System for International Airports*, [w:] *Emerging Directions in Embedded and Ubiquitous Computing*, red. M.K. Denko i in., Berlin 2007, s. 22–30, https://doi.org/10.1007/978-3-540-77090-9_3.
[6] Zob. M. Montanari, R.H. Campbell, *Multi-aspect security assessment of airport computer networks*, [w:] *AIAA Infotech at Aerospace 2010*, American Institute of Aeronautics and Astronautics Inc., Atlanta 2010, https://doi.org/10.2514/6.2010-3312.
[7] Zob. R. Abeyratne, *Cyber terrorism and aviation – national and international responses*, „Journal of Transportation Security" 2011, t. 4, wyd. 4, s. 337–349, https://doi.org/10.1007/s12198-011-0074-3.
[8] Zob. K. Sampigethaya, R. Poovendran, *Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport*, „Proceedings of the IEEE" 2013, t. 101, nr 8, s. 1834–1855, https://doi.org/10.1145/3432247.

2. Materiał i metody

W celu realizacji założeń badawczych przeprowadzono analizę bibliometryczną publikacji naukowych dotyczących cyberbezpieczeństwa w lotnictwie cywilnym. Analiza bibliometryczna jest metodą eksploracji i oceny dużych wolumenów danych naukowych[9]. W literaturze przedmiotu podkreśla się, że istnieją „dwa podstawowe zastosowania bibliometrii: ewaluacyjne (służące ocenie badaczy i jednostek naukowych) oraz deskryptywne (pozwalające na obserwację tendencji w rozwoju nauki i technologii, identyfikację istotnych aktorów)”[10]. W niniejszym artykule wykorzystano techniki deskryptywne, a proces badawczy składał się z etapów przedstawionych w tabeli 1.

Tabela 1. Proces badawczy

Lp.	Etapy
1	Określenie celu i problemu badawczego
2	Określenie słów kluczowych
3	Ustalenie kryteriów włączania i wyłączania
4	Wyszukiwanie i przygotowanie danych
5	Analiza danych
6	Interpretacja wyników i formułowanie wniosków

Źródło: opracowanie własne.

Zgodnie z tabelą 1 pierwszy etap obejmował sformułowanie celu i problemu badawczego, które przedstawiono we wprowadzeniu do niniejszego artykułu. Dotyczą one identyfikacji kierunków badań nad cyberbezpieczeństwem w lotnictwie cywilnym.

W kolejnym etapie wybrano słowa kluczowe, które posłużyły do opracowania zapytania do bazy Scopus. W tym celu uwzględniono terminy związane zarówno z cyberbezpieczeństwem, jak i z lotnictwem cywilnym. Do pierwszego obszaru włączono następujące pojęcia: cyberbezpieczeństwo, bezpieczeństwo cyfrowe, bezpieczeństwo informacji, cyberzagrożenia, cyberatak. Natomiast w odniesieniu do lotnictwa cywilnego wykorzystano takie słowa kluczowe jak: lotnictwo cywilne, lotnictwo komercyjne, port lotniczy, linie lotnicze, bezpieczeństwo lotnicze, ochrona lotnictwa.

Trzeci etap procesu badawczego obejmował wybór kryteriów włączania i wyłączania. Według Marty Makowskiej „kryteria włączania definiują cechy, jakie badanie musi mieć, jeżeli ma zostać włączone do przeglądu […]. Kryteria wyłączania mówią o cechach, które dyskwalifikują badania z przeglądu”[11]. Innymi słowy, elementy te są ustalane na potrzeby realizacji przyjętego celu badania oraz zapewnienia trafności i użyteczności wyników. W niniejszym badaniu przyjęto kryteria wyszczególnione w tabeli 2.

Tabela 2. Kryteria selekcji publikacji naukowych

Kryteria włączania	Kryteria wyłączania
Publikacje z okresu od stycznia 2015 r. do lipca 2025 r.	Publikacje spoza badanego okresu
Język angielski	Publikacje w innych językach niż angielski
Artykuły naukowe, artykuły przeglądowe, artykuły konferencyjne	Książki, rozdziały w książkach, przeglądy konferencji, edytoriale
Tematyka cyberbezpieczeństwa w lotnictwie cywilnym	Publikacje niezwiązane z tematem

Źródło: opracowanie własne.

[9] N. Donthu i in., *How to conduct a bibliometric analysis: An overview and guidelines*, „Journal of Business Research” 2021, t. 133, s. 285–296, https://doi.org/10.1016/j.jbusres.2021.04.070.
[10] K. Klinkiewicz, M. Żemigała, M. Mijal, *Bibliometria w zarządzaniu technologiami i badaniami naukowymi*, Ministerstwo Nauki i Szkolnictwa Wyższego, Warszawa 2012, s. 8.
[11] M. Makowska, *Przegląd systematyczny krok po kroku. Przewodnik dla początkujących badaczy reprezentujących nauki społeczne*, SGGW, Warszawa 2020, s. 52.

Tabela 2 przedstawia kryteria selekcji publikacji, które obejmują ramy czasowe, język, typ dokumentu oraz zgodność tematyczną. Zakres czasowy ustalono na okres od stycznia 2015 r. do lipca 2025 r. Wybór ten wynika zarówno ze wzrostu ilości publikacji, jak i zwiększonego zaangażowania państw, organizacji i społeczności międzynarodowej w problematykę cyberbezpieczeństwa w lotnictwie. Ponadto lata te są istotne ze względu na rozwój nowych technologii, takich jak np. Internet Rzeczy (IoT), sztuczna inteligencja (AI) czy też sieci 5G. Kolejnym kryterium włączania był język angielski, ponieważ jest on dominującym językiem publikacji dostępnych w bazie Scopus. Przyjęcie takich założeń pozwala zapewnić spójność językową analizowanego materiału. Przechodząc do typu dokumentów w badaniu, uwzględniono artykuły naukowe, przeglądowe i konferencyjne. Publikacje te zawierają często najnowsze wyniki badań oraz stanowią zweryfikowane i recenzowane źródła wiedzy. Inne typy pominięto z uwagi na ich ograniczoną dostępność bądź brak procesu recenzji w niektórych opracowaniach. Ostatnie kryterium miało na celu zapewnienie zgodności tematycznej z celem i problem badawczym. W badaniu uwzględniono wyłącznie publikacje dotyczące cyberbezpieczeństwa w lotnictwie cywilnym, natomiast pominięto publikacje dotyczące innej problematyki.

Po ustaleniu opisanych wyżej założeń następnym etapem było wyszukiwanie oraz przygotowanie danych. W tym celu sformułowano zapytanie do bazy Scopus, które przedstawiono w tabeli 3.

Tabela 3. Zapytanie do bazy Scopus

```
(TITLE-ABS-KEY ("cybersecurity" OR "cyber security" OR "information security" OR "digital security" OR "cyber threat" OR "cyber threats" OR "cyberattack" OR "cyberattacks" OR "cyber attack" OR "cyber attacks"))
AND (TITLE-ABS-KEY ("civil aviation" OR "commercial aviation" OR "airport" OR "airports" OR "airline" OR "airlines" OR "aviation safety" OR "aviation security"))
AND (PUBYEAR > 2014 AND PUBYEAR < 2026)
AND (DOCTYPE(ar) OR DOCTYPE(re) OR DOCTYPE(cp))
AND (LANGUAGE(english))
```

Źródło: opracowanie własne.

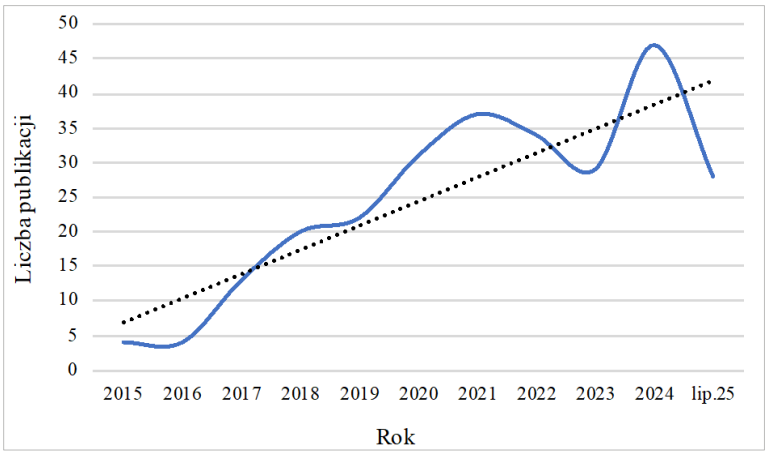
Powyższe zapytanie obejmowało ustalone słowa kluczowe z obszaru lotnictwa cywilnego i cyberbezpieczeństwa. Aby uzyskać reprezentatywną bazę danych i zwiększyć zakres wyszukiwania, uwzględniono różne warianty zapisu słów kluczowych oraz ich synonimy. Przyjęte terminy były wyszukiwane w tytule, streszczeniu oraz słowach kluczowych publikacji. Ponadto określono ramy czasowe, język publikacji oraz typ dokumentu. W wyniku wyszukiwania baza Scopus zwróciła 299 rekordów spełniających przyjęte kryteria. Następnie przeprowadzono manualną weryfikację, która polegała na sprawdzeniu tytułów, streszczeń i słów kluczowych. W wyniku selekcji odrzucono 30 pozycji ze względu na ich niezgodność tematyczną z celem badania. Ostatecznie do dalszej analizy wybrano 269 publikacji naukowych.

Etap analizy danych polegał na szczegółowym badaniu zgromadzonego zbioru publikacji. W tym celu zastosowano analizę bibliometryczną, która umożliwiła identyfikację kluczowych trendów i kierunków badań nad cyberbezpieczeństwem w lotnictwie cywilnym. Uzyskane wyniki stanowiły podstawę do realizacji ostatniego etapu, czyli interpretacji wyników oraz formułowania wniosków końcowych.

3. Wyniki badań

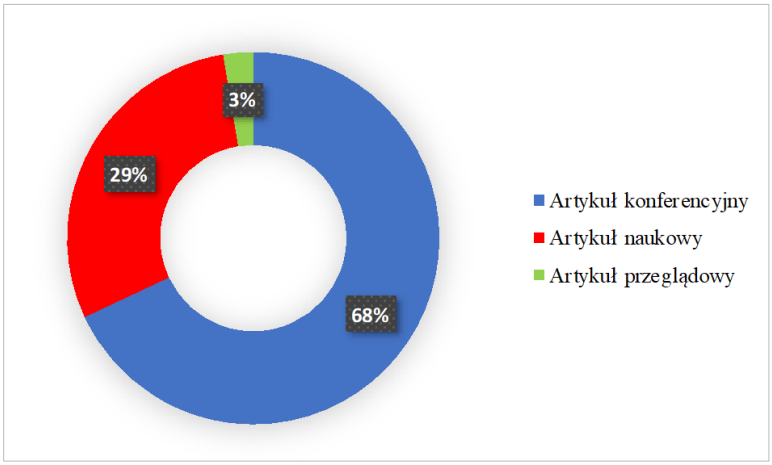
3.1. Charakterystyka publikacji

W niniejszej sekcji zaprezentowano wyniki analizy bibliometrycznej literatury naukowej. Badania oparto na 269 publikacjach zindeksowanych w bazie Scopus, które opublikowano w okresie od stycznia 2015 r. do lipca 2025 r. Pierwsza analiza dotyczy liczby publikacji w poszczególnych latach, co pozwala zaobserwować dynamikę rozwoju badań nad cyberbezpieczeństwem w lotnictwie cywilnym (wykres 1).



Wykres 1. Liczba publikacji w okresie od stycznia 2015 r. do lipca 2025 r.
Źródło: opracowanie własne na podstawie danych z bazy Scopus.

Wykres 1 prezentuje liczbę publikacji na temat cyberbezpieczeństwa w lotnictwie cywilnym. Widocznym trendem w badanym okresie jest wzrost liczby publikacji naukowych. W 2015 r. opublikowano 4 prace, natomiast w 2024 r. liczba ta wyniosła 47. Oznacza to niemalże dwunastokrotny wzrost liczby dokumentów. W latach 2021–2022 nastąpił spadek ilości publikacji. Można przypuszczać, że było to spowodowane pandemią COVID-19, która znacząco wpłynęła na funkcjonowanie sektora lotniczego i jednostek naukowych. Od 2023 r. systematycznie rosła aktywność publikacyjna, co odzwierciedla intensyfikację badań nad nowymi wyzwaniami dotyczącymi cyberbezpieczeństwa w lotnictwie cywilnym. Należy podkreślić, że dane za rok 2025 są niepełne, jednakże linia trendu sugeruje dalszy wzrost zainteresowania analizowaną problematyką. W badaniu uwzględniono również podział na typ dokumentu. Wyniki przedstawiono na wykresie 2.

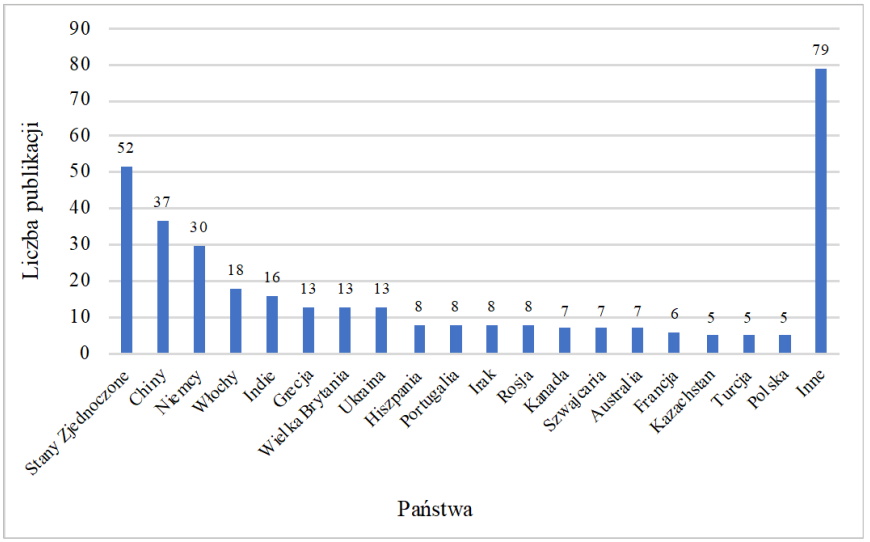


Wykres 2. Rozkład procentowy publikacji według typu
Źródło: opracowanie własne na podstawie danych z bazy Scopus.

Zgodnie z wykresem 2 największy udział w ogólnej liczbie publikacji mają artykuły konferencyjne, tj. 68% (183 pozycje). Kolejną co do wielkości grupą są artykuły naukowe, które stanowią 29% (79 publikacji). Najmniejszy odsetek posiadają artykuły przeglądowe, stanowiące jedynie 3%

(7 pozycji). Wyniki dowodzą dużej aktywności konferencyjnej, co może świadczyć o innowacyjności problematyki cyberbezpieczeństwa w lotnictwie cywilnym. Natomiast niewielka liczba artykułów przeglądowych sugeruje stosunkowo wczesną fazę rozwoju badań.

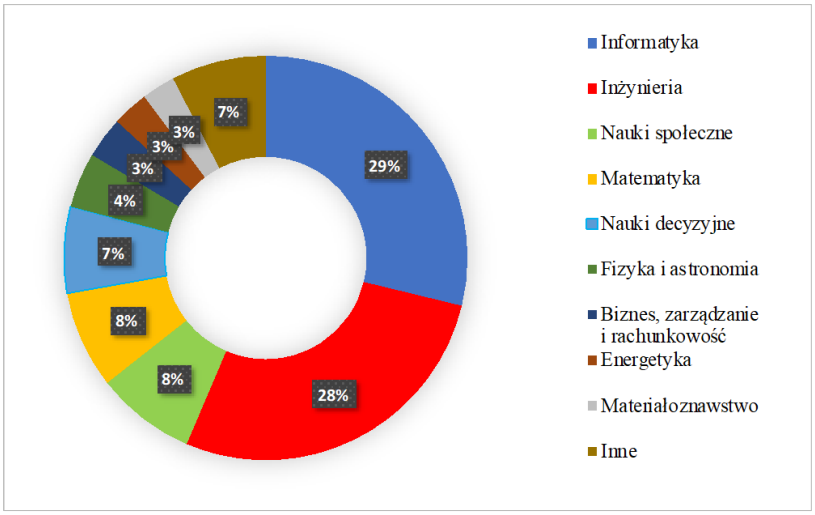
Kolejny aspekt dotyczy rozkładu publikacji według państw, co zostało przedstawione na wykresie 3. Zestawienie umożliwia identyfikację państw, które wykazują największą aktywność publikacyjną.



Wykres 3. Liczba publikacji według państw
Źródło: opracowanie własne na podstawie danych z bazy Scopus.

Według danych z bazy Scopus publikacje dotyczące cyberbezpieczeństwa w lotnictwie pochodzą z 62 krajów. W celu zapewnienia czytelności na wykresie 3 uwzględniono państwa, posiadające co najmniej 5 prac. Natomiast pozostałe zostały ujęte w zbiorczej kategorii „inne". Zgodnie z danymi Stany Zjednoczone posiadają dominującą pozycję w aktywności publikacyjnej w analizowanym obszarze (52 prace). Znaczący wkład mają także Chiny (37 publikacji) oraz Niemcy (30 publikacji). W dalszej kolejności znajdują się Włochy i Indie, z których pochodzi odpowiednio 18 i 16 publikacji. W przypadku Grecji, Wielkiej Brytanii i Ukrainy odnotowano po 13 prac. W następnej części zestawienia znajdują się państwa, które posiadają znacznie niższą liczbę publikacji. Wyniki badań dowodzą, że publikacje pochodzą z wielu państw, co może świadczyć o rosnącym, globalnym trendzie zainteresowania omawianą problematyką. Przy czym większość publikacji pochodzi z Ameryki Północnej, Europy oraz Chin, co wskazuje na koncentrację badań w regionach o rozwiniętym sektorze lotniczym i technologicznym.

W dalszym etapie uwzględniono również rozkład publikacji według dziedzin zgodnie z klasyfikacją przyjętą w bazie Scopus (wykres 4). Pozwala to określić, które obszary tematyczne dominują w badanym zbiorze publikacji.



Wykres 4. Rozkład publikacji według dziedzin
Źródło: opracowanie własne na podstawie danych z bazy Scopus.

W oparciu o dane przedstawione na wykresie 4 największy odsetek przypada na publikacje z zakresu informatyki (29%) i inżynierii (28%), które łącznie stanowią ponad połowę wszystkich pozycji. Kolejne znaczące grupy to opracowania z nauk społecznych (8%), matematyki (8%) oraz nauk decyzyjnych (7%). Mniejszy udział procentowy posiadają publikacje z dziedzin: fizyka i astronomia (4%), biznes, zarządzanie i rachunkowość (3%), energetyka (3%) oraz materiałoznawstwo (3%). Pozostałe dziedziny reprezentują najmniejszą ilość publikacji i zostały zebrane w zbiorczej kategorii „inne". Przedstawione wyniki badań wskazują na dominującą rolę publikacji z nauk technicznych, co może świadczyć o dużym zainteresowaniu rozwojem technologii oraz wysokim ich potencjale wdrożeniowym. Ponadto obecność wielu innych dziedzin potwierdza interdyscyplinarny charakter badań dotyczących cyberbezpieczeństwa w lotnictwie cywilnym.

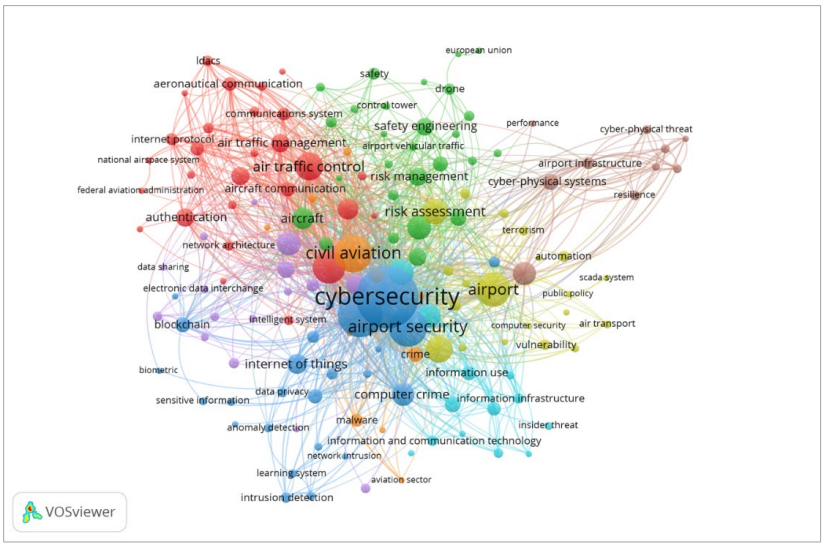
3.2. Analiza współwystępowania słów kluczowych

Zasadniczym elementem badań była analiza współwystępowania słów kluczowych. W literaturze przedmiotu podkreśla się, że:

> metoda ta polega na wykrywaniu terminów występujących w tytułach, abstraktach lub treści dwóch lub więcej różnych publikacji łącznie […]. Wykrycie powtarzających się współwystąpień pewnych fraz w różnych, rozdzielonych okresach pozwala domniemywać, że reprezentowane przez to słownictwo trendy, koncepcje lub teorie zostały zaakceptowane przez społeczność naukową[12].

Analizę współwystępowania słów kluczowych przeprowadzono z wykorzystaniem oprogramowania VOSviewer. Przyjęto, że z 2079 słów kluczowych występujących w bazie danych zostaną uwzględnione te, które wystąpiły co najmniej cztery razy. Rezultaty przedstawiono na rysunku 1.

[12] Ł. Opaliński, *Bibliometryczna metodologia prognozowania i oceny rozwoju dyscyplin naukowych. Analiza piśmiennictwa. Część 1. Publikacje pionierskie, metoda powiązań bibliograficznych, metoda współcytowań i metoda współwystępowania specjalistycznej terminologii naukowej*, „Zagadnienia Informacji Naukowej. Studia Informacyjne" 2017, t. 55, nr 1(109), s. 34–65, https://doi.org/10.36702/zin.348.



Rysunek 1. Mapa współwystępowania słów kluczowych
Źródło: opracowanie własne na podstawie danych z bazy Scopus.

W wyniku przeprowadzonej analizy wyodrębniono osiem klastrów badawczych. Wskazują one dominujące kierunki badań nad cyberbezpieczeństwem w lotnictwie cywilnym w okresie od stycznia 2015 r. do lipca 2025 r. Poszczególne klastry badawcze wraz z wybranymi słowami kluczowymi przedstawiono w tabeli 4.

Tabela 4. Klastry badawcze

Klastry	Słowa kluczowe
Klaster 1 czerwony	Międzynarodowa Organizacja Lotnictwa Cywilnego (ICAO), kontrola ruchu powietrznego, zarządzanie ruchem lotniczym, nawigacja lotnicza, łączność lotnicza, łączność statku powietrznego, cyfrowa awionika, LDACS, architektura sieci, protokół internetowy, uwierzytelnianie, kryptografia, kryptografia klucza publicznego[13]
Klaster 2 zielony	Unia Europejska, bezpieczeństwo, zarządzanie ryzykiem, inżynieria bezpieczeństwa, zapobieganie wypadkom, ruch pojazdów na lotnisku, statek powietrzny, dron, wieża kontroli lotów, ADS-B[14]
Klaster 3 niebieski	Cyberbezpieczeństwo, ochrona portu lotniczego, informacje wrażliwe, Internet Rzeczy (IoT), Blockchain, sztuczna inteligencja (AI), głębokie uczenie, biometryczny, przestępczość komputerowa, wykrywanie włamań, wykrywanie anomalii[15]
Klaster 4 żółty	Transport lotniczy, port lotniczy, automatyzacja, system SCADA, cyberatak, terroryzm, podatność[16]
Klaster 5 fioletowy	Zarządzanie informacją, podejmowanie decyzji, Big Data, udostępnianie danych, elektroniczna wymiana danych, kontrola dostępu, system czasu rzeczywistego, interoperacyjność[17]

[13] Słowa kluczowe w języku angielskim: *International Civil Aviation Organization* (ICAO), *air traffic control*, *air traffic management*, *air navigation*, *aeronautical communication*, *aircraft communication*, *digital*, *avionics*, LDACS (*L-band Digital Aeronautical Communications System*), *network, architecture*, *internet protocol*, *authentication*, *cryptography*, *public key cryptography*.
[14] Słowa kluczowe w języku angielskim: *European Union*, *safety*, *safety engineering*, *accident prevention*, *risk management, airport vehicular traffic*, *aircraft*, *drone*, *control tower*, ADS-B (*Automatic Dependent Surveillance-Broadcast).*
[15] Słowa kluczowe w języku angielskim: *cybersecurity*, *airport security*, *sensitive information*, *internet of things*, *artificial intelligence*, *blockchain*, *deep learning*, *biometric*, *computer crime*, *intrusion detection*, *anomaly detection*.
[16] Słowa kluczowe w języku angielskim: *air transport*, *airport*, *automation*, SCADA *system*, *cyber-attack*, *terrorism*, *vulnerability*.
[17] Słowa kluczowe w języku angielskim: *information management*, *decision making*, *big data*, *data sharing*, *electronic data interchange*, *access control*, *real-time system*, *interoperability*.

Klaster 6 jasnoniebieski	Lotnictwo, przemysł lotniczy, infrastruktura informacyjna, technologia informacyjno- -komunikacyjna, bezpieczeństwo danych, zagrożenie wewnętrzne, wykorzystanie informacji, edukacja[18]
Klaster 7 pomarańczowy	Lotnictwo cywilne, bezpieczeństwo informacji, przestępczość, złośliwe oprogramowanie[19]
Klaster 8 brązowy	Infrastruktura krytyczna, infrastruktura lotniska, system cyberfizyczny, zagrożenie cyberfizyczne, odporność, wydajność, autonomiczny agent, metoda obliczeniowa, symulacja propagacji[20]

Źródło: opracowanie własne.

Tabela 4 przedstawia osiem klastrów badawczych i słowa kluczowe, które określają dominujące zagadnienia badawcze dotyczące cyberbezpieczeństwa w lotnictwie cywilnym. Następną sekcję poświęcono szczegółowej charakterystyce każdego z klastrów, co pozwoli na zidentyfikowanie głównych kierunków badań.

3.3. Charakterystyka klastrów badawczych

Pierwszy klaster odnosi się do zagadnień takich jak standaryzacja oraz bezpieczeństwo systemów komunikacji, nawigacji i zarządzania ruchem lotniczym. Problematyka ta jest kluczowa dla lotnictwa cywilnego, ponieważ dotyczy zarówno zagadnień regulacyjnych, jak i technologicznych.

Odnosząc się do aspektów prawnych, należy podkreślić fundamentalne znaczenie regulacji i standardów w zapewnieniu bezpieczeństwa cyberprzestrzeni. Na zagadnienie to zwraca uwagę Michał Klenka, który wskazuje rolę instrumentów międzynarodowych oraz identyfikuje przyszłe wyzwania dla cyberbezpieczeństwa w lotnictwie cywilnym[21]. Z kolei inna praca skupia się na holistycznym wdrażaniu rozwiązań na rzecz bezpieczeństwa informacji w branży lotniczej w oparciu o normę ISO/IEC 27001[22]. Badania te są szczególnie istotne dla sektora lotniczego, ponieważ podstawy prawne i standardy warunkują skuteczność wdrażanych rozwiązań w zakresie cyberbezpieczeństwa.

Znaczącym obszarem tematycznym jest również zarządzanie ruchem lotniczym (ATM), w tym kontrola ruchu lotniczego (ATC). Terrence Lewis i współautorzy opracowali architekturę cyberbezpieczeństwa dla systemów ATM, która opiera się na zapewnieniu atrybutów bezpieczeństwa informacji, tj. poufności, integralności i dostępności. Autorzy wykorzystali modelowanie do identyfikacji zagrożeń występujących w poszczególnych fazach lotu w celu przedstawienia rekomendacji dotyczących cyberbezpieczeństwa[23]. Wyniki badań wskazują, że zapewnienie wysokiego poziomu bezpieczeństwa jest warunkiem niezbędnym do prawidłowego funkcjonowania systemów zarządzania ruchem lotniczym.

Równolegle prowadzone są również badania dotyczące systemów komunikacji i nawigacji. W tym kontekście, prace koncentrują się na analizie cyberbezpieczeństwa systemów nawigacyjnych[24] oraz na

[18] Słowa kluczowe w języku angielskim: *aviation*, *aviation industry*, *information infrastructure*, *information and communication technology*, *security of data*, *insider threat, information use, engineering education*.
[19] Słowa kluczowe w języku angielskim: *civil aviation*, *information security*, *crime*, *malware*.
[20] Słowa kluczowe w języku angielskim: *critical infrastructure*, *airport infrastructure*, *cyber-physical system*, *cyber-physical threat*, *resilience*, *performance*, *computational method*, *autonomous agent*, *propagation simulation*.
[21] M. Klenka, *Aviation cyber security: legal aspects of cyber threats*, „Journal of Transportation Security" 2021, t. 14, s. 177–195, https://doi.org/10.1007/s12198-021-00232-8.
[22] T. Salmenpää, *Information Security Governance in Civil Aviation*, [w:] *Cyber Security. Computational Methods in Applied Sciences*, red. M. Lehto, P. Neittaanmäki, Springer, Cham 2022, s. 315–336.
[23] T. Lewis, A. Hassan, K. Freeman, *Developing a Cybersecurity Architecture for Extensible Traffic Management (xTM)*, [w:] *AIAA Science and Technology Forum and Exposition*, Orlando 2025, https://doi.org/10.2514/6.2025-2720.
[24] Zob. I. Ostroumov, N. Kuzmenko, *Cybersecurity Analysis of Navigation Systems in Civil Aviation*, [w:] *2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO)*, Kijów 2022, s. 478–483, https://doi.org/10.1109/ELNANO54667.2022.9927038.

wymaganiach bezpieczeństwa i badaniu podatności systemów komunikacji lotniczej[25]. Dużą uwagę poświęca się nowoczesnym systemom łączności lotniczej, takim jak LDACS. Przykładowo, w jednej z publikacji zaproponowano środki bezpieczeństwa w celu ochrony danych w kanałach sterowania LDACS oraz oceniono ich wpływ na bezpieczeństwo i wydajność[26]. Istotne znaczenie mają także badania dotyczące rozwiązań kryptograficznych, które umożliwiają bezpieczne uwierzytelnianie i transmisję danych[27]. Podsumowując, czerwony klaster koncentruje się na regulacyjnych i technologicznych fundamentach cyberbezpieczeństwa w lotnictwie cywilnym.

Kolejną grupą wymienioną w tabeli 4 jest klaster zielony. Jego główne kierunki badań obejmują zarządzanie ryzykiem, inżynierię bezpieczeństwa oraz działania mające na celu utrzymanie wysokiego poziomu bezpieczeństwa operacyjnego. Zgodnie z przeprowadzoną analizą współwystępowania słów kluczowych zarządzanie ryzykiem jest jednym z centralnych zagadnień omawianego klastra. Veselin Monev analizuje regulacje unijne, w tym przepisy EASA Part-IS, które regulują wdrażanie systemu zarządzania bezpieczeństwem informacji oraz zarządzanie ryzykiem w sektorze lotniczym[28]. Natomiast Ahmed Elmarady i Kamel Rahouma zaproponowali systematyczną metodologię oceny ryzyka cyberbezpieczeństwa dla infrastruktury krytycznej w systemach lotniczych. Wyniki tych badań wskazują na zróżnicowane poziomy ryzyka w obrębie poszczególnych systemów komunikacji, nawigacji i nadzoru, co wymaga zastosowania adekwatnych środków ochrony[29]. Publikacje podkreślają znaczenie wdrażania systemowego zarządzania ryzykiem na potrzeby skutecznej ochrony przed cyberzagrożeniami.

Istotną rolę odgrywają również badania w obszarze inżynierii bezpieczeństwa, które obejmują projektowanie, wdrażanie oraz eksploatację systemów służących zapewnieniu wysokiego poziomu cyberbezpieczeństwa w lotnictwie cywilnym. Przy czym większość pozycji koncentruje się na praktycznych aspektach implementowanych rozwiązań. Przykładowo w jednej z prac przedstawiono podejście do oceny bezpieczeństwa oparte na modelach (MBSA) w celu projektowania koncepcyjnego systemów lotniczych. W publikacji wykazano, że zastosowanie proponowanego podejścia przynosi wiele korzyści związanych z generowaniem bezpiecznej architektury systemowej[30]. Ponadto w literaturze przedmiotu można także odnaleźć artykuły przeglądowe dotyczące teorii bezpieczeństwa i niezawodności w lotnictwie[31].

[25] Zob. N. Mäurer i in., *Security in Digital Aeronautical Communications A Comprehensive Gap Analysis*, „International Journal of Critical Infrastructure Protection" 2022, t. 38, https://doi.org/10.1016/j.ijcip.2022.100549.
[26] N. Mäurer, T. Gräupl, C. Schmitt, *Efficient Control-Channel Security for the Aeronautical Communications System LDACS*, [w:] *Proceedings – 2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston 2023, s. 407–412, https://doi.org/10.1109/WoWMoM57956.2023.00072.
[27] Zob. N. Mäurer i in., *Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS*, [w:] *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, San Antonio 2020, s. 1–10, https://doi.org/10.1109/DASC50938.2020.9256746.
[28] V. Monev, *Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)*, [w:] *2024 International Conference on Information Technologies (InfoTech)*, Sofia 2024, s. 1–4, https://doi.org/10.1109/InfoTech63258.2024.10701382.
[29] A.A. Elmarady, K. Rahouma, *Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment*, „IEEE Access" 2021, t. 9, s. 143997–144016, https://doi.org/10.1109/ACCESS.2021.3121230.
[30] S. Gradel, B. Aigner, E. Stumpf, *Model-based safety assessment for conceptual aircraft systems design*, „CEAS Aeronautical Journal" 2022, t. 13, s. 281–294, https://doi.org/10.1007/s13272-021-00562-2.
[31] Zob. N. Muecklich i in., *Safety and reliability in aviation – A systematic scoping review of normal accident theory, high-reliability theory, and resilience engineering in aviation*, „Safety Science" 2023, t. 162, https://doi.org/10.1016/j.ssci.2023.106097.

Publikacje w ramach klastra obejmują również inne zagadnienia powiązane z bezpieczeństwem operacyjnym. Część pozycji dotyczy cyberbezpieczeństwa technologii wspierających zapobieganie wypadkom, takich jak system ADS-B, który umożliwia określenie pozycji statku powietrznego w czasie rzeczywistym[32]. Stosunkowo nowym kierunkiem badań jest cyberbezpieczeństwo bezzałogowych statków powietrznych (BSP), których rosnąca liczba wymaga opracowania odpowiednich standardów interoperacyjności i zarządzania ryzykiem. W odpowiedzi na te wyzwania Trung Tran i współautorzy zaproponowali rozszerzenie metodyki oceny ryzyka SORA o elementy związane z cyber-bezpieczeństwem w operacjach z wykorzystaniem BSP[33]. Z kolei Mariusz Pyzyński i Tomasz Balcerzak przedstawili potencjalne zagrożenia związane z rosnącym wykorzystaniem dronów, omówili przykłady rzeczywistych cyberataków oraz ocenili stan regulacji prawnych. Na tej podstawie autorzy sformułowali rekomendacje obejmujące np. wdrażanie szkoleń, kampanii informacyjnych, wymiany informacji o zagrożeniach[34]. Reasumując, klaster zielony dostarcza wiedzę o cyberbezpieczeństwie w lotnictwie cywilnym ze szczególnym uwzględnieniem zarządzania ryzykiem, inżynierii bezpieczeństwa oraz bezpieczeństwa operacyjnego.

Trzeci klaster porusza zagadnienia nowych technologii na rzecz cyberbezpieczeństwa w lotnictwie cywilnym. Dominującym kierunkiem badań jest Internet Rzeczy (IoT), który odgrywa kluczową rolę w rozwoju tzw. inteligentnych lotnisk. Jak słusznie zauważają Nickolaos Koroniotis i współautorzy, IoT umożliwia integrację różnorodnych urządzeń i systemów, a także bieżące monitorowanie infrastruktury, optymalizację procesów oraz zarządzanie operacjami w czasie rzeczywistym. Jednocześnie autorzy zwracają uwagę na konieczność zapewnienia cyberbezpieczeństwa wdrażanych rozwiązań[35]. Również wiele innych pozycji zostało poświęconych problematyce bezpieczeństwa IoT w lotnictwie cywilnym. Przykładowo, w badaniu Georgii Lykou i współautorów oceniono poziom zabezpieczeń inteligentnych lotnisk oraz wskazano kluczowe podatności i zagrożenia związane z rozwojem technologii IoT[36].

W kontekście bezpieczeństwa Internetu Rzeczy coraz częściej rozważa się integrację z technologią Blockchain. Według badań Mosladdin Shueb i współautorów, Blockchain w systemach IoT dla lotnictwa cywilnego może znacząco zwiększyć odporność na cyberataki oraz ograniczyć awarie[37]. Blockchain może znaleźć również zastosowanie m.in. w systemach monitorowania infrastruktury, rejestrach operacji, zarządzaniu dostępem oraz w systemach uwierzytelniania użytkowników. W literaturze podkreśla się także możliwości tej technologii w zarządzaniu ruchem lotniczym (ATM). W publikacji Xin Lu i współautorów zaproponowano architekturę opartą na technologii Blockchain w celu zapewnienia wiarygodności, bezpieczeństwa i dostępności informacji w systemach ATM[38]. Wyniki

[32] Zob. M.A. Rahman, T. Bhuiyan, M. Ameer Ali, *Enhancing aviation safety: Machine learning for real-time ADS-B injection detection through advanced data analysis*, „Alexandria Engineering Journal" 2025, t. 126, s. 262–276, https://doi.org/10.1016/j.aej.2024.10.042.

[33] T.D. Tran i in., *Toward Cybersecurity of Unmanned Aircraft System operations under "Specific" category*, [w:] *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*, Ateny 2020, s. 1433–1441, https://doi.org/10.1109/ICUAS48674.2020.9213903.

[34] M. Pyzynski, T. Balcerzak, *Cybersecurity of the Unmanned Aircraft System (UAS)*, „IEEE Access" 2021, t. 102, wyd. 2, nr 35, s. 1–13, https://doi.org/10.1007/s10846-021-01399-x.

[35] N. Koroniotis i in., *A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports*, „IEEE Access" 2020, t. 8, s. 209802–209834, https://doi.org/10.1109/ACCESS.2020.3036728.

[36] G. Lykou, A. Anagnostopoulou, D. Gritzalis, *Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls*, „Sensors" 2019, t. 19, wyd. 1, https://doi.org/10.3390/s19010019.

[37] M.M. Shueb, C. Yang, X. Che, *An Innovative Design for Improving U.S. Airports Cybersecurity Based on Blockchain Technology*, [w:] *Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, Charlottesville 2024, s. 232–237, https://doi.org/10.1109/SIEDS61124.2024.10534684.

[38] X. Lu, Z. Wu, J. Cao, *ATMChain: Blockchain-Based Security Architecture for Air Traffic Management in Future,* „IEEE Transactions on Aerospace and Electronic Systems" 2024, t. 60, nr 4, s. 3872–3896, https://doi.org/10.1109/taes.2024.3371396.

badań wskazują, że zaprojektowane rozwiązanie wykazuje potencjał w zakresie zwiększenia poziomu cyberbezpieczeństwa w lotnictwie cywilnym.

Istotnym wyzwaniem identyfikowanym w literaturze jest wzrost cyberprzestępczości[39]. Trend ten wpływa na rozwój badań naukowych w zakresie zaawansowanej analizy danych opartej na sztucznej inteligencji (AI) i uczeniu maszynowym, w tym technikach głębokiego uczenia[40]. Publikacje są w szczególności ukierunkowane na detekcję włamań[41] oraz wykrywanie anomalii[42]. Ponadto można także odnaleźć pozycje odnoszące się do konkretnych rodzajów cyberataków charakterystycznych dla lotnictwa cywilnego. Przykładowo, Vajratiya Vajrobol i współautorzy zaprojektowali system do wykrywania ataków polegających na wstrzykiwaniu fałszywych danych do systemów ADS-B (ang. *ADS-B injection*)[43]. Z kolei inni badacze opracowali rozwiązanie oparte na głębokim uczeniu się do detekcji ataków typu DDoS w sieciach 5G w lotnictwie[44]. Warto podkreślić, że praktyczne podejście przedstawione w przywołanych badaniach pełni ważną rolę w szybkim reagowaniu na incydenty bezpieczeństwa.

Znaczącym nurtem badawczym są także biometryczne systemy kontroli dostępu. Cechy biometryczne, w tym układ naczyń krwionośnych palca, mogą stanowić skuteczny element ochrony fizycznej portów lotniczych[45]. Z drugiej zaś strony, wykorzystanie technik biometrycznych wymaga zapewnienia ochrony informacji wrażliwych. Badania w tym zakresie koncentrują się na integracji biometrii z rozwiązaniami kryptograficznymi i technologią Blockchain, co może przyczynić się do skutecznego zabezpieczenia informacji w branży lotniczej[46]. Podsumowując, publikacje w klastrze niebieskim obejmują rozwój nowych technologii na rzecz zapewnienia cyberbezpieczeństwa w lotnictwie cywilnym. Główne kierunki badań to monitorowanie infrastruktury, wykrywanie anomalii, detekcja zagrożeń oraz ochrona danych wrażliwych.

Przechodząc do charakterystyki pozostałych klastrów badawczych, należy podkreślić, że dotyczą one zagadnień rzadziej podejmowanych w literaturze. Klaster żółty porusza zagadnienia bezpieczeństwa systemów automatyzacji i sterowania przemysłowego w sektorze transportu lotniczego. Literatura wskazuje, że rozwój zautomatyzowanych rozwiązań, takich jak systemy SCADA, prowadzi do

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

[40] Zob. A.B. Garcia, R.F. Babiceanu, R. Seker, *Artificial Intelligence and Machine Learning Approaches For Aviation Cybersecurity: An Overview*, [w:] *Integrated Communications Navigation and Surveillance Conference (ICNS)*, IEEE, Dulles 2021, s. 1–8, https://doi.org/10.1109/ICNS52807.2021.9441594.

[41] Zob. B. Sezari, D.P.F. Möller, A. Deutschmann, *Anomaly-Based Network Intrusion Detection Model Using Deep Learning in Airports*, [w:] *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, Nowy Jork 2018, s. 1725–1729, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00261.

[42] Zob. J. Jevčák i in., *Innovative software tool for cyber security against security incidents in civil aviation network operations*, [w:] *New Trends in Aviation Development (NTAD)*, red. R. Andoga, L. Fozo, IEEE, Stary Smokowiec 2024, s. 73–78, https://doi.org/10.1109/NTAD63796.2024.10850485.

[43] V. Vajrobol i in., *Enhancing aviation control security through ADS-B injection detection using ensemble meta-learning models with Explainable AI*, „Alexandria Engineering Journal" 2025, t. 122, s. 63–73, https://doi.org/10.1016/j.aej.2024.10.042.

[44] H. Whitworth i in., *5G Aviation Networks Using Novel AI Approach for DDoS Detection*, „IEEE Access" 2023, t. 11, s. 77518–77542, https://doi.org/10.1109/ACCESS.2023.3296311.

[45] D.P. Wagh, H.S. Fadewar, G.N. Shinde, *Biometric Finger Vein Recognition Methods for Authentication*, [w:] *Advances in Intelligent Systems and Computing*, red. B. Iyer i in., Springer, Aurangabad 2019, s. 45–53, https://doi.org/10.1007/978-981-32-9515-5_5.

[46] O. Malek i in., *Fusion of blockchain and biometrics: an integrated platform for aviation security and authentication*, [w:] *Proceedings of SPIE – The International Society for Optical Engineering*, red. M. Blowers, R.D. Hall, V.R. Dasari, SPIE, Orlando 2022, https://doi.org/10.1117/12.2624966.

pojawienia się nowych wyzwań w zakresie cyberbezpieczeństwa[47]. W związku z tym, opracowanie narzędzi do wykrywania podatności w tych systemach stanowi istotny obszar badań w lotnictwie cywilnym[48]. Klaster podkreśla znaczenie ochrony systemów automatyzacji i sterowania przemysłowego, gdyż są one niezbędne do zapewnienia ciągłości operacji lotniczych.

Klaster fioletowy koncentruje się na zagadnieniach zarządzania informacją oraz interoperacyjności systemów. W obliczu rosnącej ilości danych skuteczna i bezpieczna ich wymiana jest jednym z kluczowych wyzwań dla lotnictwa cywilnego. W tym kontekście Madhu Niraula zwraca uwagę na zagadnienia związane z zapewnieniem interoperacyjności systemów komunikacyjnych różnych podmiotów sektora lotniczego[49]. Jednym z rozwiązań wspierających systemowe zarządzanie informacją w lotnictwie cywilnym jest SWIM (ang. *System Wide Information Management*), który umożliwia standaryzowaną wymianę danych pomiędzy interesariuszami. Przy czym, jak słusznie sądzą Xiaodong Lu i Naoki Kanada, zapewnienie cyberbezpieczeństwa wymaga kompleksowego zarządzania zaufaniem w ramach SWIM, które obejmuje cyfrową tożsamość, odporność sieciową, zarządzanie dostępem oraz zarządzanie ryzykiem[50]. Ponadto coraz większą rolę w zarządzaniu informacją w lotnictwie cywilnym odgrywają technologie Big Data, umożliwiające przetwarzanie i analizę heterogenicznych zbiorów danych. Jednak rozwiązania te również wymagają zastosowania zaawansowanych mechanizmów cyberbezpieczeństwa[51]. Klaster odnosi się zatem do istotnych dla lotnictwa zagadnień związanych z efektywnym zarządzaniem informacją przy jednoczesnym zapewnieniu bezpieczeństwa.

Kolejny klaster dotyczy przemysłu lotniczego i infrastruktury informacyjnej. Jednym z poruszanych w literaturze zagadnień badawczych są technologie przełomowe w przemyśle lotniczym. Badania Edisy Dreković i współautorów pokazują, że przyczyniają się one do zwiększenia efektywności operacyjnej i obniżenia kosztów. Niemniej jednak proces ich implementacji wiąże się z wyzwaniami w zakresie optymalizacji, integracji z istniejącymi systemami, zgodności z przepisami, a także cyberbezpieczeństwem[52]. Również przegląd zgłoszeń patentowych wskazuje na rozwój innowacji w obszarze technologii informacyjno-komunikacyjnych stosowanych w sektorze lotniczym, w tym także związanych z ochroną portu lotniczego[53]. Publikacje uwzględniają również znaczenie czynnika

[47] Zob. O. Milbredt i in., *Aviation security automation: The current level of security automation and its impact*, „Journal of Airport Management" 2022, t. 16, wyd. 2, s. 184–208, https://doi.org/10.69554/ZFKK4145.
[48] Zob. L. Gong i in., *Civil Aviation Industrial Control Systems Vulnerability Mining Based on Fuzzing Technology*, [w:] *IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, red. H. Sun, IEEE, Dali 2023, s. 580–584, https://doi.org/10.1109/ICCASIT58768.2023.10351714.
[49] M. Niraula, *Cybersecurity and Interoperability of Aviation Safety Service Ecosystem*, [w:] *Integrated Communication, Navigation and Surveillance Conference (ICNS)*, Dulles 2022, s. 1–12, https://doi.org/10.1109/ICNS54818.2022.9771482.
[50] X. Lu, N. Kanada, *SWIM Service Trust Framework to Ensure the Safety of Flight Operations*, [w:] *2023 IEEE 12th Global Conference on Consumer Electronics (GCCE)*, Nara 2023, s. 485–486, https://doi.org/10.1109/GCCE59613.2023.10315499.
[51] Zob. D. Miltiadou i in., *Big Data Intelligence Marketplace and Secure Analytics Experimentation Platform for the Aviation Industry*, [w:] *Big Data Technologies and Applications*, red. Z. Deze i in., Springer, Cham 2020, s. 48–62, https://doi.org/10.1007/978-3-030-72802-1_4.
[52] E. Dreković, Ž. Teofilović, I. Karabegović, *The Application of Disruptive Technologies in the Aviation Industry*, [w:] *New Technologies, Development and Application VIII*, red. I. Karabegović, A. Kovačević, S. Mandžuka, Springer, Cham 2025, s. 602–611, https://doi.org/10.1007/978-3-031-95194-7_63.
[53] M. Eleimat, O. Alharasees, A. Oszi, *Advancements in Airport Security Technologies: A Patent Analysis*, [w:] *Mediterranean Smart Cities Conference (MSCC)*, red. A.B. Dahmane, A. El Hibaoui, M. Essaaidi, IEEE, Martil–Tetuan 2024, s. 1–5, https://doi.org/10.1109/MSCC62288.2024.10696990.

ludzkiego i szkoleń[54], a także zagrożeń wynikających z błędu lub celowych działań pracowników[55]. Przywołane badania koncentrują się na istotnej tematyce związanej z rozwojem przemysłu lotniczego oraz odpowiednim przygotowaniem personelu.

Klaster pomarańczowy obejmuje literaturę dotyczącą bezpieczeństwa informacji w lotnictwie cywilnym. Badania odnoszą się do przestępczości i wykorzystania złośliwego oprogramowania do ataków wymierzonych w systemy teleinformatyczne branży lotniczej[56]. Klaster ten podkreśla rosnącą rolę ochrony informacji w lotnictwie cywilnym jako elementu szerszego podejścia do cyberbezpieczeństwa w tym sektorze.

Ostatni klaster dotyczy ochrony infrastruktury krytycznej, w tym w szczególności aspektów związanych z ochroną fizyczną. W odniesieniu do tej tematyki Shivendra Anand i Madhavi Dave omówili znaczenie cyberbezpieczeństwa portów lotniczych jako kluczowych elementów infrastruktury krytycznej. Według autorów, zastosowanie technik prewencyjnych może być pomocne w podejmowaniu proaktywnych działań na rzecz skutecznego zapobiegania cyberatakom[57]. Badania w tym klastrze skupiają się również na bezpieczeństwie systemów cyberfizycznych (CPS), które integrują komponenty cyfrowe i fizyczne w celu umożliwienia monitorowania i kontroli w czasie rzeczywistym[58]. Ponadto publikacje podejmują problematykę odporności infrastruktury lotniskowej oraz metod wykrywania cyberzagrożeń[59].

Analiza współwystępowania słów kluczowych umożliwiła identyfikację ośmiu klastrów badawczych, które określają dominujące kierunki badań nad cyberbezpieczeństwem w lotnictwie cywilnym występujące w okresie od stycznia 2015 r. do lipca 2025 r. Scharakteryzowane grupy tematyczne obejmują szerokie spektrum poruszanych zagadnień, w tym aspekty prawne, techniczne, fizyczne i dotyczące czynnika ludzkiego.

4. Zakończenie

Celem artykułu była identyfikacja i charakterystyka głównych kierunków badań nad cyberbezpieczeństwem w lotnictwie cywilnym. Założenie to zrealizowano na podstawie literatury zindeksowanej w bazie Scopus, która została opublikowana w okresie od stycznia 2015 r. do lipca 2025 r. W kontekście prowadzonych rozważań sformułowano następujące wnioski:

1. Analiza bibliometryczna wykazała, że cyberbezpieczeństwo stało się w ostatnich latach jednym z kluczowych obszarów zainteresowania środowiska naukowego zajmującego się sektorem lotniczym. Porównując dane z 2015 r. i 2024 r., można zauważyć niemal dwunastokrotny wzrost liczby publikacji, co wskazuje na dynamiczny rozwój tej problematyki. Ponadto dominującą formą publikacji są artykuły konferencyjne, co może świadczyć o innowacyjności tematu. Natomiast

[54] Zob. R. Sabillon, J.R. Bermejo-Higuera, *The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities*, [w:] *International 2023 – Late Breaking Papers. HCII 2023. Lecture Notes in Computer Science*, red. H. Degen, S. Ntoa, A. Moallem, Springer, Cham 2023, s. 461–479, https://doi.org/10.1007/978-3-031-48057-7_29.
[55] Zob. J. Fielding, *The people problem: how cyber security's weakest link can become a formidable asset*, „Computer Fraud and Security" 2020, nr 1, s. 6–9, https://doi.org/10.1016/S1361-3723(20)30006-3.
[56] L. Florido-Benítez, *The types of hackers and cyberattacks in the aviation industry*, „Journal of Transportation Security" 2024, t. 17, nr 13, https://doi.org/10.1007/s12198-024-00281-9.
[57] S. Anand, M. Dave, *Cybersecurity Resiliency for Airports as a Critical Infrastructure*, [w:] *Lecture Notes in Electrical Engineering*, red. S.J. Patel i in., Springer, Singapur 2024, s. 1–16, https://doi.org/10.1007/978-981-99-5091-1_1.
[58] Q.U. Ain i in., *Anomaly Detection for Aviation Cyber-Physical System: Opportunities and Challenges*, „IEEE Access" 2024, t. 12, s. 175905–175925, https://doi.org/10.1109/ACCESS.2024.3495519.
[59] Zob. C. Köpke i in., *Resilience Quantification for Critical Infrastructure: Exemplified for Airport Operations*, [w:] *Computer Security. ESORICS 2021 International Workshops*, red. S. Katsikas i in., Spiringer, Cham 2020, s. 451–460, https://doi.org/10.1007/978-3-030-95484-0_26.

niewielki udział artykułów przeglądowych podkreśla potrzebę dalszej systematyzacji wiedzy w omawianym obszarze.

2. Największa aktywność publikacyjna występuje w Stanach Zjednoczonych, Chinach i krajach europejskich, czyli państwach o rozwiniętym sektorze lotniczym oraz znaczącym potencjale badawczo-rozwojowym. Z drugiej zaś strony, udział ponad 60 państw w analizowanym dorobku wskazuje na rosnące i globalne zainteresowanie problematyką cyberbezpieczeństwa w lotnictwie cywilnym. Struktura dziedzinowa odzwierciedla wyraźną przewagę publikacji z obszaru nauk technicznych, co może sugerować ukierunkowanie badań na aspekty technologiczne i wdrożeniowe. Z kolei występowanie wielu innych dyscyplin potwierdza interdyscyplinarny i złożony charakter przedmiotu badań.
3. Analiza współwystępowania słów kluczowych umożliwiła wyodrębnienie ośmiu klastrów, które określają główne kierunki badań. Wyniki wskazują na potrzebę przyjęcia holistycznego podejścia do cyberbezpieczeństwa w branży lotniczej, które łączy elementy prawne, techniczne, organizacyjne, fizyczne oraz związane z czynnikiem ludzkim. Poruszane zagadnienia obejmują zarówno kwestie fundamentalne, takie jak standaryzacja systemów lotniczych, jak i nowe technologie (np. Internet Rzeczy, Big Data, sztuczna inteligencja, Blockchain). Publikacje odnoszą się również do innych rozwiązań praktycznych np. ochrona infrastruktury krytycznej, detekcja zagrożeń, zarządzanie ryzykiem, dobór zabezpieczeń. Innymi słowy, zidentyfikowane klastry obrazują złożoność badań oraz silne ich powiązanie z rozwojem nowych technologii.
4. Przeprowadzona analiza ujawniła także luki badawcze, które wymagają pogłębionej eksploracji. Jak już wcześniej wspomniano, liczba prac przeglądowych jest stosunkowo niewielka, co utrudnia systematyzację wiedzy i wskazuje na potrzebę ich opracowania. Dane zwracają uwagę na niedostateczny rozwój badań nad wpływem czynnika ludzkiego na cyberbezpieczeństwo w lotnictwie cywilnym. Dotyczy to w szczególności szkoleń i kształtowania kultury cyberbezpieczeństwa. Z perspektywy przyszłych prac szczególnie istotne wydają się zagadnienia związane z zarządzaniem ryzykiem wynikającym z integracji nowych technologii. Kluczowe w tym zakresie są takie elementy jak: analiza podatności, identyfikacja zagrożeń oraz dobór środków minimalizujących ryzyko. Ponadto rozwój inteligentnych portów lotniczych czy też bezzałogowych statków powietrznych wymaga dalszych badań w zakresie interoperacyjności, standaryzacji i zapewnienia zgodności z regulacjami prawnymi.

Podsumowując, cyberbezpieczeństwo w lotnictwie cywilnym można uznać za jeden z kluczowych obszarów, którego znaczenie będzie prawdopodobnie systematycznie rosło w kolejnych latach. Przegląd literatury wskazuje na trend wzrostowy liczby publikacji, interdyscyplinarność i globalny zasięg zagadnienia. Uzyskane wyniki mogą stanowić podstawę do dalszych badań lub analiz porównawczych z innymi bazami danych, np. Web of Science (WoS).

BIBLIOGRAFIA

Artykuły i monografie

Abeyratne R., *Cyber terrorism and aviation – national and international responses*, „Journal of Transportation Security" 2011, t. 4, wyd. 4, https://doi.org/10.1007/s12198-011-0074-3.

Ain Q.U. i in., *Anomaly Detection for Aviation Cyber-Physical System: Opportunities and Challenges*, „IEEE Access" 2024, t. 12, https://doi.org/10.1109/ACCESS.2024.3495519.

Anand S., Dave M., *Cybersecurity Resiliency for Airports as a Critical Infrastructure*, [w:] *Lecture Notes in Electrical Engineering*, red. S.J. Patel i in., Springer, Singapur 2024, https://doi.org/10.1007/978-981-99-5091-1_1.

Chang H. i in., *The Case Study of Information Security System for International Airports*, [w:] *Emerging Directions in Embedded and Ubiquitous Computing*, red. M.K. Denko i in., Berlin 2007, https://doi.org/10.1007/978-3-540-77090-9_3.

Donthu N. i in., *How to conduct a bibliometric analysis: An overview and guidelines*, „Journal of Business Research" 2021, t. 133, https://doi.org/10.1016/j.jbusres.2021.04.070.

Dreković E., Teofilović Ž., Karabegović I., *The Application of Disruptive Technologies in the Aviation Industry*, [w:] *New Technologies, Development and Application VIII*, red. I. Karabegović, A. Kovačević, S. Mandžuka, Springer, Cham 2025, https://doi.org/10.1007/978-3-031-95194-7_63.

Eleimat M., Alharasees O., Oszi A., *Advancements in Airport Security Technologies: A Patent Analysis*, [w:] *Mediterranean Smart Cities Conference (MSCC)*, red. A.B. Dahmane, A. El Hibaoui, M. Essaaidi, IEEE, Martil–Tetuan 2024, https://doi.org/10.1109/MSCC62288.2024.10696990.

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

Fielding J., *The people problem: how cyber security's weakest link can become a formidable asset*, „Computer Fraud and Security" 2020, nr 1, https://doi.org/10.1016/S1361-3723(20)30006-3.

Florido-Benítez L., *The types of hackers and cyberattacks in the aviation industry*, „Journal of Transportation Security" 2024, t. 17, nr 13, https://doi.org/10.1007/s12198-024-00281-9.

Garcia A.B., Babiceanu R.F., Seker R., *Artificial Intelligence and Machine Learning Approaches For Aviation Cybersecurity: An Overview*, [w:] *Integrated Communications Navigation and Surveillance Conference (ICNS)*, IEEE, Dulles 2021, https://doi.org/10.1109/ICNS52807.2021.9441594.

Global Aviation Security Plan (GASeP), Doc 10118, ICAO 2024.

Gong L. i in., *Civil Aviation Industrial Control Systems Vulnerability Mining Based on Fuzzing Technology*, [w:] *IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, red. H. Sun, IEEE, Dali 2023, https://doi.org/10.1109/ICCASIT58768.2023.10351714.

Gradel S., Aigner B., Stumpf E., *Model-based safety assessment for conceptual aircraft systems design*, „CEAS Aeronautical Journal" 2022, t. 13, https://doi.org/10.1007/s13272-021-00562-2.

Jevčák J. i in., *Innovative software tool for cyber security against security incidents in civil aviation network operations*, [w:] *New Trends in Aviation Development (NTAD)*, red. R. Andoga, L. Fozo, IEEE, Stary Smokowiec 2024, https://doi.org/10.1109/NTAD63796.2024.10850485.

Klenka M., *Aviation cyber security: legal aspects of cyber threats*, „Journal of Transportation Security" 2021, t. 14, https://doi.org/10.1007/s12198-021-00232-8.

Klinkiewicz K., Żemigała M., Mijal M., *Bibliometria w zarządzaniu technologiami i badaniami naukowymi*, Ministerstwo Nauki i Szkolnictwa Wyższego, Warszawa 2012.

Köpke C. i in., *Resilience Quantification for Critical Infrastructure: Exemplified for Airport Operations*, [w:] *Computer Security. ESORICS 2021 International Workshops*, red. S. Katsikas i in., Spiringer, Cham 2020, https://doi.org/10.1007/978-3-030-95484-0_26.

Koroniotis N. i in., *A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports*, „IEEE Access" 2020, t. 8, https://doi.org/10.1109/ACCESS.2020.3036728.

Lewis T., Hassan A., Freeman K., *Developing a Cybersecurity Architecture for Extensible Traffic Management (xTM)*, [w:] *AIAA Science and Technology Forum and Exposition*, Orlando 2025, https://doi.org/10.2514/6.2025-2720.

Lu X., Kanada N., *SWIM Service Trust Framework to Ensure the Safety of Flight Operations*, [w:] *2023 IEEE 12th Global Conference on Consumer Electronics (GCCE)*, Nara 2023, https://doi.org/10.1109/GCCE59613.2023.10315499.

Lu X., Wu Z., Cao J., *ATMChain: Blockchain-Based Security Architecture for Air Traffic Management in Future*, „IEEE Transactions on Aerospace and Electronic Systems" 2024, t. 60, nr 4, https://doi.org/10.1109/taes.2024.3371396.

Lykou G., Anagnostopoulou A., Gritzalis D., *Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls*, „Sensors" 2019, t. 19, wyd. 1, https://doi.org/10.3390/s19010019.

Makowska M., *Przegląd systematyczny krok po kroku. Przewodnik dla początkujących badaczy reprezentujących nauki społeczne*, SGGW, Warszawa 2020.

Malek O. i in., *Fusion of blockchain and biometrics: an integrated platform for aviation security and authentication*, [w:] *Proceedings of SPIE – The International Society for Optical Engineering*, red. M. Blowers, R.D. Hall, V.R. Dasari, SPIE, Orlando 2022, https://doi.org/10.1117/12.2624966.

Mäurer N. i in., *Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS*, [w:] *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC*), San Antonio 2020, https://doi.org/10.1109/DASC50938.2020.9256746.

Mäurer N. i in., *Security in Digital Aeronautical Communications A Comprehensive Gap Analysis*, „International Journal of Critical Infrastructure Protection" 2022, t. 38, https://doi.org/10.1016/j.ijcip.2022.100549.

Mäurer N., Gräupl T., Schmitt C., *Efficient Control-Channel Security for the Aeronautical Communications System LDACS*, [w:] *Proceedings – 2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston 2023, https://doi.org/10.1109/WoWMoM57956.2023.00072.

Milbredt O. i in., *Aviation security automation: The current level of security automation and its impact*, „Journal of Airport Management" 2022, t. 16, wyd. 2, https://doi.org/10.69554/ZFKK4145.

Miltiadou D. i in., *Big Data Intelligence Marketplace and Secure Analytics Experimentation Platform for the Aviation Industry*, [w:] *Big Data Technologies and Applications*, red. Z. Deze i in., Springer, Cham 2020, https://doi.org/10.1007/978-3-030-72802-1_4.

Monev V., *Aviation Safety within an Information Security Risk Management Process (EASA Part-IS)*, [w:] *2024 International Conference on Information Technologies (InfoTech)*, Sofia 2024, https://doi.org/10.1109/InfoTech63258.2024.10701382.

Montanari R., Campbell R.H., *Multi-aspect security assessment of airport computer networks*, [w:] *AIAA Infotech at Aerospace 2010*, American Institute of Aeronautics and Astronautics Inc., Atlanta 2010, https://doi.org/10.2514/6.2010-3312.

Muecklich N. i in., *Safety and reliability in aviation – A systematic scoping review of normal accident theory, high-reliability theory, and resilience engineering in aviation*, „Safety Science" 2023, t. 162, https://doi.org/10.1016/j.ssci.2023.106097.

Niraula M., *Cybersecurity and Interoperability of Aviation Safety Service Ecosystem*, [w:] *Integrated Communication, Navigation and Surveillance Conference (ICNS)*, Dulles 2022, https://doi.org/10.1109/ICNS54818.2022.9771482.

Opaliński Ł., *Bibliometryczna metodologia prognozowania i oceny rozwoju dyscyplin naukowych. Analiza piśmiennictwa. Część 1. Publikacje pionierskie, metoda powiązań bibliograficznych, metoda współcytowań i metoda współwystępowania specjalistycznej terminologii naukowej*, „Zagadnienia Informacji Naukowej. Studia Informacyjne" 2017, t. 55, nr 1(109), https://doi.org/10.36702/zin.348.

Ostroumov I., Kuzmenko N., *Cybersecurity Analysis of Navigation Systems in Civil Aviation*, [w:] *2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO*), Kijów 2022, https://doi.org/10.1109/ELNANO54667.2022.9927038.

Pyzynski M., Balcerzak T., *Cybersecurity of the Unmanned Aircraft System (UAS)*, „IEEE Access" 2021, t. 102, wyd. 2, nr 35, https://doi.org/10.1007/s10846-021-01399-x.

Rahman M.A., Bhuiyan T., Ameer Ali M., *Enhancing aviation safety: Machine learning for real-time ADS-B injection detection through advanced data analysis*, „Alexandria Engineering Journal" 2025, t. 126, https://doi.org/10.1016/j.aej.2024.10.042.

Rinaldi S.M., Peerenboom J.P., Kelly T.K., *Identifying, understanding, and analyzing critical infrastructure interdependencies*, „IEEE Control Systems Magazine" 2001, t. 21, nr 6, https://doi.org/10.1109/37.969131.

Sabillon R., Bermejo-Higuera J.R., *The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities*, [w:] *International 2023 – Late Breaking Papers. HCII 2023. Lecture Notes in Computer Science*, red. H. Degen, S. Ntoa, A. Moallem, Springer, Cham 2023, https://doi.org/10.1007/978-3-031-48057-7_29.

Salmenpää T., *Information Security Governance in Civil Aviation*, [w:] *Cyber Security. Computational Methods in Applied Sciences*, red. M. Lehto, P. Neittaanmäki, Springer, Cham 2022.

Sampigethaya K., Poovendran R., *Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport*, „Proceedings of the IEEE" 2013, t. 101, nr 8, https://doi.org/10.1145/3432247.

Sezari A., Möller DP.F., Deutschmann A., *Anomaly-Based Network Intrusion Detection Model Using Deep Learning in Airports*, [w:] *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, IEEE, Nowy Jork 2018, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00261.

Shueb M.M., Yang C., Che X., *An Innovative Design for Improving U.S. Airports Cybersecurity Based on Blockchain Technology*, [w:] *Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, Charlottesville 2024, https://doi.org/10.1109/SIEDS61124.2024.10534684.

Tran T.D. i in., *Toward Cybersecurity of Unmanned Aircraft System operations under "Specific" category*, [w:] *2020 International Conference on Unmanned Aircraft Systems (ICUAS)*, Ateny 2020, https://doi.org/10.1109/ICUAS48674.2020.9213903.

Vajrobol V. i in., *Enhancing aviation control security through ADS-B injection detection using ensemble meta-learning models with Explainable AI*, „Alexandria Engineering Journal" 2025, t. 122, https://doi.org/10.1016/j.aej.2024.10.042.

Wagh D.P., Fadewar H.S., Shinde G.N., *Biometric Finger Vein Recognition Methods for Authentication*, [w:] *Advances in Intelligent Systems and Computing*, red. B. Iyer i in., Springer, Aurangabad 2019, https://doi.org/10.1007/978-981-32-9515-5_5.

Whitworth H. i in., *5G Aviation Networks Using Novel AI Approach for DDoS Detection*, „IEEE Access" 2023, t. 11, https://doi.org/10.1109/ACCESS.2023.3296311.

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

Źródła internetowe

https://www.google.com/maps/d/embed?mid=1ptVIma0CZqoPiN-zsomzbRVQDRS7BXGk [dostęp: 30.06.2025].

https://www.icao.int/icao-global-aviation-security-plan-gasep [dostęp: 30.06.2025].