miesięcznik naukowo-techniczny Wydawnictwa SITK RP sp. z o.o.

przegląd komunikacyjny

5
2023
rocznik LXXVIII
cena 27,00 zł
w tym 8% VAT

UKAZUJE SIĘ OD 1945 ROKU

Cyberbezpieczeństwo infrastruktury krytycznej

eISSN
2544-6037

ISSN
0033-22-32

Cyberbezpieczeństwo systemów uzbrojenia sił powietrznych Stanów Zjednoczonych - zapewnienie bezpieczeństwa misji. Cyberbezpieczeństwo a rewolucja cyfrowa (na przykładzie domeny cywilnej i wojskowej). Zagrożenia cyberbezpieczeństwa dla infrastruktury lotniczej. Infrastruktura krytyczna a odporność strategiczna państwa. Drogowe odcinki lotniskowe jako element infrastruktury krytycznej i obronnej państwa

Podstawowe informacje dla Autorów artykułów

„Przegląd Komunikacyjny" publikuje artykuły związane z szeroko rozumianym transportem oraz infrastrukturą transportu. Obejmuje to zagadnienia techniczne, ekonomiczne i prawne. Akceptowane są także materiały związane z geografią, historią i socjologią transportu.

Artykuły publikowane w „Przeglądzie Komunikacyjnym" dzieli się na: „wnoszące wkład naukowy w dyscypliny: inżynieria lądowa i transport; ekonomia i finanse; nauki prawne; nauki socjologiczne. Prosimy Autorów o deklarację (w zgłoszeniu), do której dyscypliny zaliczyć ich prace.

Materiały do publikacji: zgłoszenie, artykuł oraz oświadczenie Autora, należy przesyłać w formie elektronicznej na adres redakcji:

artykuly@przeglad.komunikacyjny.pwr.wroc.pl

W zgłoszeniu należy podać: imię i nazwisko autora, adres mailowy oraz adres do tradycyjnej korespondencji, miejsce zatrudnienia, zdjęcie, tytuł artykułu oraz streszczenie (po polsku i po angielsku) i słowa kluczowe (po polsku i po angielsku). Szczegóły przygotowania materiałów oraz wzory załączników dostępne są ma stronie:

www.transportation.overview.pwr.edu.pl

W celu usprawnienia i przyspieszenia procesu publikacji prosimy o zastosowanie się do poniższych wymagań dotyczących nadsyłanego materiału:

1. Tekst artykułu powinien być napisany w jednym z ogólnodostępnych programów (np. Microsoft Word). Wzory i opisy wzorów powinny być wkomponowane w tekst. Tabele należy zestawić po zakończeniu tekstu. Ilustracje (rysunki, fotografie, wykresy) najlepiej dołączyć jako oddzielne pliki. Można je także wstawić do pliku z tekstem po zakończeniu tekstu. Możliwe jest oznaczenie miejsc w tekście, w których autor sugeruje wstawienie stosownej ilustracji lub tabeli. Obowiązuje odrębna numeracja ilustracji (bez rozróżniania na rysunki, fotografie itp.) oraz tabel.
2. Całość materiału nie powinna przekraczać 12 stron w formacie Word (zalecane jest 8 stron). Do limitu stron wlicza się ilustracje załączane w odrębnych plikach (przy założeniu że 1 ilustracja = ½ strony).
3. Format tekstu powinien być jak najprostszy (nie stosować zróżnicowanych styli, wcięć, podwójnych i wielokrotnych spacji itp.). Dopuszczalne jest pogrubienie, podkreślenie i oznaczenie kursywą istotnych części tekstu, a także indeksy górne i dolne. **Nie stosować przypisów.**
4. Nawiązania do pozycji zewnętrznych - cytaty (dotyczy również podpisów ilustracji i tabel) oznacza się numeracją w nawiasach kwadratowych [...]. Numerację należy zestawić na końcu artykułu (jako „Materiały źródłowe"). Zestawienie powinno być ułożone alfabetycznie.
5. Jeżeli Autor wykorzystuje materiały objęte nie swoim prawem autorskim, powinien uzyskać pisemną zgodę właściciela tych praw do publikacji (niezależnie od podania źródła). Kopie takiej zgody należy przesłać Redakcji.

Artykuły wnoszące wkład naukowy w dyscypliny: inżynieria lądowa i transport, inżynieria lądowa i transport; ekonomia i finanse; nauki prawne; nauki socjologiczne podlegają procedurom recenzji merytorycznych zgodnie z wytycznymi MNiSW, co pozwala zaliczyć je, po opublikowaniu, do dorobku naukowego oraz uwzględnić w ewaluacji jakości działalności naukowej (Dz.U. 2019 poz. 392).

Liczba uwzględnianych punktów wg listy czasopism punktowanych przez MNiSW wynosi 20.

Do oceny każdej publikacji powołuje się co najmniej dwóch niezależnych recenzentów spoza jednostki. Zasady kwalifikowania lub odrzucenia publikacji i ewentualny formularz recenzencki są podane do publicznej wiadomości na stronie internetowej czasopisma lub w każdym numerze czasopisma. Nazwiska recenzentów poszczególnych publikacji/numerów nie są ujawniane.

Przygotowany materiał powinien obrazować własny wkład badawczy autora. Redakcja wdrożyła procedurę zapobiegania zjawisku Ghostwriting (z „ghostwriting" mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, bez ujawnienia swojego udziału jako jeden z autorów lub bez wymienienia jego roli w podziękowaniach zamieszczonych w publikacji). Tekst i ilustracje muszą być oryginalne i niepublikowane w innych miejscach (w tym w internecie). Możliwe jest zamieszczanie artykułów, które ukazały się w materiałach konferencyjnych i podobnych (na prawach rękopisu) z zaznaczeniem tego faktu i po przystosowaniu do wymogów publikacyjnych „Przeglądu Komunikacyjnego".

Na stronie internetowej czasopisma dostępne są pełne wersje artykułów wraz ze streszczeniami w języku polskim (od 2010) i angielskim (od 2016) jako OPEN ACCESS. Pod koniec 2018 roku „Przegląd Komunikacyjny" rozpoczął indeksowanie artykułów angielskich z użyciem numerów cyfrowych DOI. Czasopismo ubiega się o partycypowanie w bazie SCOPUS. Rejestrowane jest w międzynarodowej baza DOAJ https://doaj.org/.

Redakcja pisma oferuje objęcie patronatem medialnym konferencji, debat, seminariów itp.
Ceny są negocjowane indywidualnie w zależności od zakresu zlecenia. Możliwe są atrakcyjne upusty. Patronat obejmuje:

- ogłaszanie przedmiotowych inicjatyw na łamach pisma,
- zamieszczanie wybranych referatów / wystąpień po dostosowaniu ich do wymogów redakcyjnych,
- publikację informacji końcowych (podsumowania, apele, wnioski),
- kolportaż powyższych informacji do wskazanych adresatów.

www.transportation.overview.pwr.edu.pl

Ramowa oferta dla „Sponsora strategicznego" czasopisma Przegląd Komunikacyjny

Sponsor strategiczny zawiera umowę z wydawcą czasopisma na okres roku kalendarzowego z możliwością przedłużenia na kolejne lata. Uprawnienia wydawcy do zawierania umów posiada Spółka Wydawnictwa SITK RP sp. z o.o..

Przegląd Komunikacyjny oferuje dla sponsora strategicznego następujące świadczenia:

- **zamieszczenie logo sponsora w każdym numerze,**
- **zamieszczenie reklamy sponsora w jednym, kilku lub we wszystkich numerach,**
- **publikacja jednego lub kilku artykułów sponsorowanych,**
- **publikacja innych materiałów dotyczących sponsora,**
- **zniżki przy zamówieniu prenumeraty czasopisma.**

Możliwe jest także zamieszczenie materiałów od sponsora na stronie internetowej czasopisma.
Przegląd Komunikacyjny ukazuje się jako miesięcznik.
Szczegółowy zakres świadczeń oraz detale techniczne (formaty, sposób i terminy przekazania) są uzgadniane indywidualnie.

Osoba kontaktowa w tej sprawie:
Hanna Szary
hanna.szary@sitkrp.org.pl
ul. Świętokrzyska 14 A , lok. 150 , 00-050 Warszawa, tel.: (22) 336 12 06, 506 116 966

Cena za świadczenia na rzecz sponsora uzależniana jest od uzgodnionych szczegółów współpracy. Zapłata może być dokonana jednorazowo lub w kilku ratach (na przykład kwartalnych). Część zapłaty może być w formie zamówienia określonej liczby prenumerat czasopisma.

przegląd komunikacyjny 5/2023 rocznik LXXVIII

Na okładce: "*Cyberbezpieczeństwo*" *(Pexels)*

Szanowni P.T. Czytelnicy

Przekazujemy kolejny numer Przeglądu Komunikacyjnego, jest on poświęcony cyberbezpieczeństwu infrastruktury technicznej. W pierwszym artykule Autor przedstawia założenia dotyczące zagrożenia systemów uzbrojenia sił powietrznych które obecnie są w znacznym stopniu uzależnione od skomplikowanego oprogramowania i dużej ilości wzajemnych powiązań w celu realizacji misji bojowych. Autor wskazuje iż celem tworzenia nowych rozwiązań jest, wypracowanie takiego rozwiązania, aby państwa oraz zainteresowane strony były w stanie opracować podejście typu system systemów (system-of-systems), które umożliwi ochronę przed zagrożeniami cybernetycznymi oraz reagowanie na incydenty cybernetyczne i usuwanie ich skutków w odpowiednim czasie, a tym samym zwiększenie odporności na nowe zagrożenia bez znaczących zakłóceń użycia systemów walki. W kolejnym artykule Autor wskazuje, że największe potęgi militarne na świecie na pierwszym miejscu stawiają cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpracę z pilotowanymi samolotami lub załogowymi okrętami, sztuczną inteligencją oraz wykorzystaniu przestrzeni kosmicznej i cyberprzestrzeni. Należy tu podkreślić, ze podjęte działania pozwalają prowadzić działania bojowe w czasie rzeczywistym. Powstaje świat zdeformowany poznawczo w którym trudno jest ocenić obiektywnie zaistniałe sytuacje. Bowiem inaczej oceniają sytuację Stany Zjednoczone, a inaczej Europa, inaczej Chiny i Rosja. W trzecim artykule Autorka przedstawia zagadnienia cyberbezpieczeństwa w lotnictwie cywilnym oraz główne kierunki działań organów nadzoru nad lotnictwem cywilnym światowego ICAO oraz europejskiego EASA. Autorka przedstawia wiodące dokumenty oraz dotychczasowe działania podjęte w kwestiach zapewnienia cyberbezpieczeństwa w zakresie ochrony danych wszystkich uczestników rynku lotniczego opracowane na szczeblu międzynarodowym. Autorka wskazuje inicjatywy ICAO i EASA odnoszące się do cyberprzestrzeni, potrzebę skoordynowania krajowych regulacji z odpowiednimi przepisami dotyczącymi zarządzania bezpieczeństwem i ochroną danych oraz włączenia cyberbezpieczeństwa do państwowych systemów nadzoru nad bezpieczeństwem i ochroną lotnictwa jako części kompleksowych ram zarządzania ryzykiem. W artykule przedstawione zostały również przykłady cyberincydentów w branży lotniczej w kontekście zdarzeń monitorowanych przez Eurocontrol oraz zalecenia dotyczące poprawy zdolności przewidywania, wykrywania, reagowania i łagodzenia cyberzagrożeń w lotnictwie cywilnym. W kolejnym artykule Autor wskazuje jak w ostatnim okresie pandemia COVID – 19 i wydarzenia związane z agresją Rosji na Ukrainę oraz ogólny wzrost napięcia w stosunkach międzynarodowych poddały surowemu sprawdzianowi systemy bezpieczeństwa globalnego, regionalnego oraz narodowego poszczególnych państw. Doświadczenia z tych wydarzeń dostarczają wielu wniosków, które powinny być wykorzystane w procesie dostosowywania systemów bezpieczeństwa do nowego i wciąż zmieniającego się środowiska polityczno – militarnego, ekonomicznego, społecznego i naturalnego. Doświadczenia te uwypukliły znaczenie odporności strategicznej państwa, a także sojuszy. Znalazło to swoje odbicie w dokumentach normatywnych zarówno narodowych jak i sojuszniczych. W Sojuszu Północnoatlantyckim powołany został Komitet Odporności jako najwyższy organ doradczy ds. odporności strategicznej oraz przygotowania społeczeństwa do funkcjonowania w czasie kryzysu i wojny. W ostatnim artykule Autorzy wskazują, że jednym z bardzo istotnych elementów infrastruktury krytycznej i obronnej Polski, obok sieci lotnisk wojskowych i cywilnych, są drogowe odcinki lotniskowe, których funkcja, znaczenie i przydatność nabrały szczególnego wymiaru w aktualnej sytuacji geopolitycznej, w tym przede wszystkim podczas trwającego konfliktu zbrojnego w Ukrainie. Drogowe odcinki lotniskowe (DOL) to specjalnie przygotowane odcinki dróg publicznych przystosowane do wykonywania operacji lotniczych startu i lądowania wojskowych statków powietrznych (WSP) realizujących zadania operacyjne w czasie kryzysu i wojny oraz zadania wynikające z realizacji procesu szkolenia lotniczego. Przedstawiono wymagania dla podstawowych parametrów eksploatacyjnych nawierzchni na obiektach użytkowanych przez służby drogowe, które należy stosować przede wszystkim: przy projektowaniu i budowie DOL.

W numerze także przegląd prasy z zakresu transportu i infrastruktury transportowej.

Życzę naszym czytelnikom dobrej lektury.

Redaktor Naczelny

Prof. Antoni Szydło

W numerze

Wydawca:
Wydawnictwa SITK RP sp. z o.o.
ul. Świętokrzyska 14 A , lok. 150 , 00-050 Warszawa
www.sitkrp.org.pl
Wawrzyniec Wychowański – Prezes

Redaktor Naczelny:
Antoni Szydło

Redakcja:
Maciej Kruszyna (Z-ca Redaktora Naczelnego), Agnieszka Kuniczuk - Trzcinowicz (Redaktor językowy), Piotr Mackiewicz (Sekretarz), Wojciech Puła (Redaktor statystyczny), Eryk Mączka (obsługa techniczna, strona internetowa), Krzysztof Gasz, Jarosław Kuźniewski, Łukasz Skotnicki, Bartłomiej Krawczyk, Igor Gisterek, Karina Korycka (obsługa anglojęzyczna)

Adres redakcji do korespondencji:
Poczta elektroniczna:
redakcja@przeglad.komunikacyjny.pwr.wroc.pl
Poczta „tradycyjna":
Piotr Mackiewicz, Maciej Kruszyna
Politechnika Wrocławska,
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
Faks: 71 320 45 39

Rada naukowa:
Marek Ciesielski (Poznań), Antanas Klibavičius (Wilno), Jozef Komačka (Žilina), Elżbieta Marciszewska (Warszawa), Andrzej S. Nowak (Auburn University), Tomasz Nowakowski (Wrocław), Victor V. Rybkin (Dniepropietrovsk), Marek Sitarz (Katowice), Wiesław Starowicz (Kraków), Hans-Christoph Thiel (Cottbus), Tomasz Siwowski (Rzeszów), Jiri Strasky (Brno), Andrea Zuzulova (Bratysława)

Deklaracja o wersji pierwotnej czasopisma
Główną wersją czasopisma jest wersja elektroniczna. Na stronie internetowej czasopisma dostępne są pełne wersje artykułów wraz ze streszczeniami w języku polskim (od 2010) i angielskim (od 2016).

Redakcja zastrzega sobie prawo dokonywania zmian w materiałach nie podlegających recenzji.

Artykuły opublikowane w „Przeglądzie Komunikacyjnym" są dostępne w bazach danych 20 bibliotek technicznych oraz są indeksowane w bazach:

BAZTECH: **http://baztech.icm.edu.pl**
Index Copernicus: **http://indexcopernicus.com**
Międzynarodowa baza DOAJ **https://doaj.org/**

Prenumerata:
Szczegóły i formularz zamówienia na stronie:
http://www.transportation.overview.pwr.edu.pl

Obecna Redakcja dysponuje numerami archiwalnymi począwszy od 4/2010.

Numery archiwalne z lat 2004-2009 można zamawiać w Oddziale krakowskim SITK, ul. Siostrzana 11, 30-804 Kraków, tel./faks 12 658 93 74, **mrowinska@sitk.org.pl**

Druk:
Grupa Intromax Sp. z o.o, ul. Biskupińska 21, 30-732 Kraków, http://www.intromax.com.pl/

Reklama:
Dział Marketingu:
hanna.szary@sitkrp.org.pl,
elzbieta.nowicka@sitkrp.com,
roman.goralski@sitkrp.com

Nakład: 800 egz.

Budowa S1. Do wojewody trafił wniosek o pozwolenie na budowę ostatniego nowego odcinka ekspresowej S1 z Mysłowic do Bierunia

Anna Dziedzic, Dziennik Zachodni, 7.05.2023

Wniosek o pozwolenie na budowę 10-kilometrowego odcinka drogi ekspresowej S1 między Mysłowicami i Bieruniem trafił do wojewody śląskiego. To efekt zakończenia prac projektowych przez wykonawcę tej, całkiem nowej części, jednej z najważniejszych dróg w regionie. Dopiero po uzyskaniu pozwolenia, będą mogły się rozpocząć prace budowlane. Mowa o części dwupasmowej trasy zaczynającej się na węźle Mysłowice Kosztowy i kończącej przed węzłem Bieruń (...). Asfaltowa dwupasmówka między Mysłowicami i Bielskiem-Białą będzie liczyła około 40 kilometrów długości. Budowę podzielono na cztery części. Tylko dwa odcinki spośród czterech mają szansę na oddanie do użytku w 2023 roku. To odcinek od węzła Oświęcim (z węzłem) do Dankowic i Dankowice Bielsko Biała (Hałcnów). Pierwszy ma być, według wstępnych założeń, gotowy 14 sierpnia 2023 r., drugi 8 listopada 2023 r (...).

Stacja kolejowa w Zawierciu będzie przebudowana. Podpisano umowę na wykonanie prac, na peronach będzie bezpieczniej i wygodniej

Paweł Kurczonek, Dziennik Zachodni, 6.05.2023

Perony na stacji kolejowej w Zawierciu doczekają się przebudowy. PKP Polskie Linie Kolejowe S.A. podpisały umowę na realizację inwestycji. - Realizowane inwestycje podnoszące parametry linii kolejowych, zwiększające bezpieczeństwo i komfort podróży sprawiają, że kolej staje się coraz bardziej konkurencyjnym środkiem transportu – mówi Andrzej Adamczyk, minister infrastruktury. Prace zakończą się w ostatnim kwartale 2024 r.

- Dla poprawy komfortu podróżnych na stacji Zawiercie zaplanowano wymianę płyt na peronach oraz budowę dwóch poczekalni otwartych z ławkami dla pasażerów. Peron przy budynku dworca zostanie wydłużony w kierunku przejścia podziemnego i skrócony od strony nastawni (zachowana zostanie jego długość 400 m) – informuje spółka (...).

Budowa S7. Kiedy pojedziemy w końcu wygodną dwupasmówką z Krakowa do Warszawy? Minimum półtora roku

Piotr Tymczak, Gazeta Krakowska, 5.05.2023

Pod koniec kwietnia oddano do użytku kolejny odcinek drogi ekspresowej S7, dzięki któremu kierowcy mogą bez przeszkód korzystać z trasy o długości 230 km pomiędzy Warszawą, Radomiem i Kielcami, aż do granicy województw świętokrzyskiego i małopolskiego. Na to, by dwupasmówką przejechać z Krakowa do stolicy trzeba jeszcze trochę poczekać. Trwają prace na trzech odcinkach między Krakowem a województwem świętokrzyskim. Ostatni z nich ma zostać oddany do użytku w listopadzie 2024 roku. W Małopolsce powstają trzy odcinki drogi ekspresowej S7: Moczydło (granica województwa świętokrzyskiego i małopolskiego) – Miechów (18,7 km), Miechów – Szczepanowice (5,3 km), Widoma – Kraków Nowa Huta (18,3 km). Pojawiły się opóźnienia na odcinku Moczydło – Miechów (...).

Ruszy budowa ważnych wiaduktów i mostów w Poznaniu. Jeszcze w maju pierwszy przetarg

Grzegorz Okoński, Głos Wielkopolski, 8.05.2023

W tym roku mają ruszyć prace nad budową dwóch ważnych dla Poznania obiektów inżynieryjnych – mostów pieszo-rowerowych nad Wartą i Cybiną na Berdychowie, a także wiaduktów drogowych na Lutyckiej i Golęcińskiej. Te ostatnie jednak wciąż będą czekały na szereg uzgodnień. Oba wiadukty mają sprawić, że mocno wzrośnie przepustowość skrzyżowań z linią kolejową Poznań – Piła, na których ruch kołowy będzie odbywał się niezależnie od ruchu kolejowego (...).

Rozpoczęły się prace na linii kolejowej Zagórz-Krościenko

PAP/Wojciech Huk, nowiny24.pl, 7.05.2023

Rozpoczęły się prace remontowe na podkarpackim odcinku linii kolejowej nr 108 Zagórz–Krościenko (granica państwa) – poinformowała PAP Dorota Szalacha z biura prasowego PKP Polskie Linie Kolejowe. Koszt prac wynosi prawie 8 mln zł. Szalacha dodała, że rozpoczęta inwestycja stanowi kontynuację prac remontowych wykonanych wcześniej na tej linii.

- Prace, które się teraz rozpoczęły mają na celu zachowanie przejezdności i zwiększenie bezpieczeństwa na odcinku od Zagórza do granicy państwa – podkreśliła. W ramach inwestycji wyremontowanych zostanie 19 obiektów inżynieryjnych, w tym 5 mostów, m.in. w Uhercach Mineralnych i Olszanicy, wiadukt w miejscowości Stefkowa oraz 13 przepustów.

- Dla podniesienia poziomu bezpieczeństwa, przewidziano także remont przejazdu kolejowo-drogowego w Ustrzykach Dolnych – zaznaczyła Szalacha. Realizacja tej inwestycji, jak dodała Szalacha, wyeliminuje lokalne ograniczenia prędkości na ośmiu obiektach inżynieryjnych (...).

Więcej pieniędzy na nowe tramwaje w Krakowie dzięki wsparciu z Unii Europejskiej

Piotr Tymczak, Gazeta Krakowska, 4.05.2023

MPK w Krakowie otrzyma ze środków unijnych 52,4 mln zł dofinansowania. Dodatkowe fundusze mają zostać uwzględnione jako wkład własny dotyczący zakupu kolejnych tramwajów Lajkonik II, których dostarczenie zaplanowano w tym roku. Centrum Unijnych Projektów Transportowych rozstrzygnęło konkurs na dofinansowanie projektów dotyczących zakupu taboru autobusowego nisko i zeroemisyjnego – z napędem elektrycznym, wodorowym lub gazowym (LNG i CNG) oraz taboru tramwajowego i trolejbusowego. MPK w Krakowie otrzyma ze środków unijnych 52,4 mln zł dofinansowania. Wniosek przygotowany przez MPK dotyczył zakupu 10 nowych tramwajów Lajkonik II, które zaczęły służyć mieszkańcom w 2022 r. – jest to element dużego kontraktu obejmującego dostawę w sumie 60 nowych Lajkoników II (...).

Pierwszy na Podkarpaciu elektryczny autobus szkolny jest już w Jaworniku Polskim

Józef Lonczak, nowiny24.pl, 5.05.2023

Jawornik Polski jest pierwszą gminą w województwie podkarpackim, która kupiła elektryczny autobus szkolny. Władze gminy Jawornik Polski w powiecie przeworskim postawiły na ekologiczny transport szkolny i zdecydowały się na zakup elektrycznego autobusu wraz z infrastrukturą do ładowania. Otrzymały na to dofinansowanie z Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej w ramach programu

„Kangur - Bezpieczna i ekologiczna droga do szkoły". - Wybraliśmy autobus ICE12 firmy Busnex Poland, ponieważ spełnia on wszystkie nasze oczekiwania i co nie mniej ważne, mieści się w budżecie zadania pod nazwą „Ochrona atmosfery - System zielonych inwestycji (GIS - Green Investment Scheme) - Kangur - Bezpieczna i ekologiczna droga do szkoły". Nasza rozbudowana punktacja przetargowa zmierzała do wyboru autobusu, który umożliwi zarówno codzienny dowóz dzieci do szkoły, jak również wyjazdy na wycieczki, zawody sportowe czy na basen - podkreśla Stanisław Petynia, wójt gminy Jawornik Polski (...).

Przystanek Kraków Zabłocie w nowej odsłonie. Perony zostały powiększone

Piotr Tymczak, Gazeta Krakowska, 4.05.2023

W ramach przebudowy linii średnicowej przecinającej Kraków zmienił się też przystanek kolejowy na Zabłociu. Został rozbudowany, by zmieściła się na nim dodatkowa para torów.
- Z zewnątrz przystanek wygląda podobnie, ale w środku sporo się zmieniło. Po obydwu stronach powstała konstrukcja ustawiona na filarach. Elewacja została odtworzona w nowym miejscu. Perony powiększono, by pociągi mogły zatrzymać się z obydwu stron. Pasażerowie mogą się schronić przed słońcem czy deszczem pod zadaszeniem. Na przystanku trwają jeszcze prace wykończeniowe. Od czerwca pociągi zaczną kursować tu po każdym z czterech torów - informują w PKP Polskie Linie Kolejowe. Inwestycja realizowana jest w ramach gigantycznego zadania za przeszło 1,2 mld zł, polegającego na dobudowie drugiej pary torów na linii kolejowej E30 na odcinku Kraków Główny Towarowy – Rudzice (...).

Lubelskiego Lipca '80 robi krok ku przedłużeniu. Miasto podpisało umowę z wykonawcą

Jakub Sarek, Kurier Lubelski, 4.05.2023

Od lutego 2025 r. kierowcy będą mogli korzystać z brakującego, ponad kilometrowego odcinka Lubelskiego Lipca'80. Dzisiaj (4 maja) ratusz poinformował o podpisaniu umowy z wykonawcą robót - firmą Strabag. Kontrakt na wykonanie prac opiewa na 96 milionów złotych. Jak tłumaczy Justyna Góźdź z biura prasowego ratusza, kolejnym krokiem po podpisaniu umowy będzie zgłoszenie rozpoczęcia prac do Wojewódzkiego Inspektora Nadzoru Budowlanego. Jeszcze w tym miesiącu miasto planuje przekazać wykonawcy plac budowy, by ten rozpoczął prace przygotowawczo-porządkowe pod przyszłą drogę. A ta zostanie przedłużona od skrzyżowania z ul. Diamentową i ul. Krochmalną do ul. Cukrowniczej. Na całej długości ma mieć dwie jezdnie i trzy pasy ruchu, z czego skrajne będą zarezerwowane dla autobusów (...).

Naczelny Sąd Administracyjny oddalił skargę kasacyjną w sprawie budowy drogi S52. GDDKiA może kontynuować przygotowania BDI.

Bogusław Kwiecień, Gazeta Krakowska, 12.05.2023

Naczelny Sąd Administracyjny oddalił skargę kasacyjną na decyzję o środowiskowych uwarunkowaniach w związku z budową drogi ekspresowej S52 Bielsko-Biała - Głogoczów nazywanej także Beskidzką Drogą Integracyjną. Na tę decyzję czekali mieszkańcy kilkunastu gmin leżących przy DK 52. Decyzja NSA oznacza, że wydana w lipcu 2018 roku przez Generalnego Dyrektora Ochrony Środowiska decyzja stała się prawomocna. GDDKiA może więc kontynuować prace przygotowawcze związane z drogą ekspresową S52 Bielsko-Biała – Głogoczów (...). Przetarg na zaprojektowanie i budowę S52 od Bielska-Białej do Głogoczowa zaplanowany jest na 2025 rok. Droga będzie budowana w ramach Rządowego Programu Budowy Dróg Krajowych do 2030 r. z perspektywą do 2033 r.

20 kilometrów nowej ścieżki rowerowej na Opolszczyźnie powstało dzięki Unii Europejskiej. Już można po niej jeździć

Mateusz Majnusz, nto.pl, 9.05.2023

Dzięki funduszom europejskim i wspólnej determinacji władz gmin Popielów i Lewin Brzeski oraz samorządu województwa wybudowano dwadzieścia kilometrów nowej ścieżki rowerowej, po której cykliści już chętnie jeżdżą (...). W Popielowie "bike&ride" usytuowano przy przystanku autobusowym, w Lewinie Brzeskim – przy stacji kolejowej. Wszystko po to, żeby w jak największym stopniu ograniczyć ruch samochodowy i żeby jak najwięcej ludzi korzystało z transportu publicznego. Cały projekt kosztował ponad 20 milionów złotych, z czego 12 milionów dopłaciła Unia Europejska (...).

Już za kilka tygodni otwarta zostanie obwodnica Olesna, czyli duży opolski odcinek drogi ekspresowej S11

Mirosław Dragon, nto.pl, 5.05.2023

Obwodnica Praszki i Gorzowa Śląskiego już jest otwarta, a dwa razy dłuższa i do tego dwupasmowa obwodnica Olesna zostanie otwarta dla kierowców za kilka tygodni (...). To największa inwestycja drogowa w historii Opolszczyzny od czasów budowy opolskiego odcinka autostrady A4. Nawet budowa obwodnicy Opola była tańsza. Nic dziwnego, skoro budowana przez opolski oddział Generalnej Dyrekcji Dróg Krajowych i Autostrad trasa obwodnicą Olesna jest tylko przy okazji. Przede wszystkim jest to 25-kilometrowy kawałek opolskiego odcinka drogi ekspresowej S11. Dla północnej Opolszczyzny ta trasa będzie tym samym, czym dla południa regionu jest autostrada A4 (...).

Drogi rowerowe we Wrocławiu pod lupą NIK. Daleko nam do najlepszych, oto największe nieprawidłowości

Konrad Bałajewicz, Gazeta Wrocławska, 11.05.2023

Wrocławska delegatura Najwyższej Izby Kontroli sprawdziła utrzymanie i rozwój infrastruktury rowerowej w 10 wybranych miastach. NIK w swoim raporcie wskazuje, że Wrocławiowi wciąż daleko do europejskiej rowerowej czołówki: Holendrów i Duńczyków (...). NIK zwróciła uwagę na nierówne nawierzchnie ścieżek rowerowych na ul. Kamiennej, Borowskiej i Komandorskiej. Wrocławscy urzędnicy obiecują, że ich stan zostanie poprawiony (...). NIK pokreśliła w raporcie nieprawidłową szerokość pasów rowerowych na ul. Małachowskiego, ul. Mickiewicza, ul. Piłsudskiego, ul. Świdnickiej, ul. Skargi oraz pl. Orląt Lwowskich. Ponadto na ul. Skargi i ul. Świdnickiej sposób wyznaczenia pasów nie spełnia wymogów określonych przepisami prawa. Wrocławscy urzędnicy tłumaczą, że w trakcie projektowania ścieżki rowerowe miały szerokość zgodną z ówczesnymi przepisami (...).

Cyberbezpieczeństwo systemów uzbrojenia sił powietrznych Stanów Zjednoczonych - zapewnienie bezpieczeństwa misji

Cybersecurity of United States Air Force Weapons Systems - ensuring mission security

Leszek Cwojdziński

Dr hab. inż. pil.

Airbus Poland S.A.

samolot221@wp.pl

Streszczenie: W niniejszym artykule zaprezentowano założenia dotyczące zagrożenia systemów uzbrojenia sił powietrznych które obecnie są w znacznym stopniu uzależnione od skomplikowanego oprogramowania i dużej ilości wzajemnych powiązań w celu realizacji misji bojowych. Zdolności cybernetyczne umożliwiają wiele zaawansowanych funkcji (np. atak elektroniczny, połączenie czujników i ich wzajemnej komunikacji), które dają lotnictwu bojowemu przewagę nad potencjalnymi przeciwnikami. Jednakże stanowią one również potencjalne możliwości i bodźce dla przeciwników do przeciwdziałania przewadze sił powietrznych poprzez ataki cybernetyczne. Autor omówił w jaki sposób wyrafinowany przeciwnik może dążyć do odkrycia i wykorzystania luk w oprogramowaniu samolotu, systemach wspomagających lub łańcuchu dostaw w celu zdobycia informacji wywiadowczych lub sabotowania operacji. Potencjalne ryzyko nie ogranicza się wyłącznie do najnowszych i najbardziej zaawansowanych system ale także do systemów które w ciągu najbliższej dekady lub dwóch będą wycofywane z eksploatacji. Starsze samoloty, które obecnie jeszcze stanowią większość zasobów US Air Force, są również narażone na ataki ze strony ewoluujących zagrożeń cybernetycznych i muszą podlegać ochronie. Audyty cyberbezpieczeństwa wykazują iż obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości dzisiejszego środowiska bezpieczeństwa cybernetycznego. Modelowa polityka bezpieczeństwa cybernetycznego ma służyć jako przewodnik pomagający państwom i ich siłom zbrojnym skupić zasoby i działania mające na celu osiągnięcie systemowego podejścia do cyberbezpieczeństwa w tym do obecnych i wprowadzanych w przyszłości systemów bojowych. Autor wskazuje iż celem tworzenia nowych rozwiązań jest, wypracowanie takiego rozwiązania, aby państwa oraz zainteresowane strony były w stanie opracować podejście typu system systemów (system-of-systems), które umożliwi ochronę przed zagrożeniami cybernetycznymi oraz reagowanie na incydenty cybernetyczne i usuwanie ich skutków w odpowiednim czasie, a tym samym zwiększenie odporności na nowe zagrożenia bez znaczących zakłóceń użycia systemów walki.

Słowa kluczowe: *Cyberbezpieczeństwo; Środowisko bezpieczeństwa; System systemów; Polityka bezpieczeństwa; Kultura bezpieczeństwa; Siły powietrzne; Lotnictwo bojowe; Systemy walki*

Abstract: This article presents assumptions about the threat to air force weapon systems which today are heavily dependent on complex software and a large number of interconnections to accomplish combat missions. Cyber capabilities enable many advanced functions (e.g., electronic attack, sensor interconnection and communications) that give combat aviation an advantage over potential adversaries. However, they also create potential opportunities and incentives for adversaries to counter the air force's superiority through cyber attacks. The author discusses how a sophisticated adversary may seek to discover and exploit vulnerabilities in aircraft software, support systems or the supply chain to gain intelligence or sabotage operations. The potential risk is not just limited to the newest and most advanced systems but also to systems that will be going out of service within the next decade or two. Older aircraft, which currently still make up the majority of US Air Force assets, are also vulnerable to attack from evolving cyber threats and must be protected. Cyber security audits show that current policies are better suited to simple, stable and predictable environments than to the complex, rapidly changing and unpredictable reality of today's cyber security environment. The model cybersecurity policy is intended to serve as a guide to help countries and their armed forces focus resources and activities to achieve a systemic approach to cyber security, including current and future combat systems being introduced. The author points out that the goal of developing new solutions is for states and stakeholders to be able to develop a systems-of-systems approach to protect against cyber threats and respond to and recover from cyber incidents in a timely manner, thereby increasing resilience to new threats without significant disruption to the use of combat systems.

Keywords: *Cyber security; Security environment; System of systems; Security policy; Security culture; Air force; Combat aviation; Combat systems*

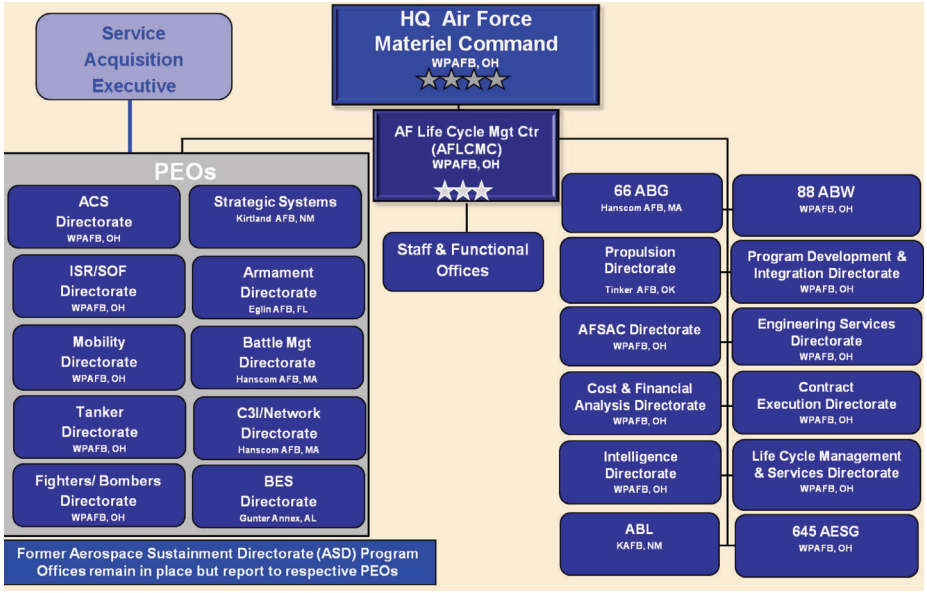
Systemy uzbrojenia Sił Powietrznych są dziś w znacznym stopniu uzależnione od skomplikowanego oprogramowania i dużej ilości wzajemnych połączeń w celu realizacji swoich misji. Zdolności cybernetyczne umożliwiają wiele zaawansowanych funkcji (np. atak elektroniczny, połączenie czujników i ich wzajemna komunikacja), które dają Siłom Powietrznym przewagę nad potencjalnymi przeciwnikami. Jednakże stwarzają one również potencjalne możliwości i bodźce dla przeciwników do przeciwdziałania przewadze USA poprzez ataki cybernetyczne. Przykładem jest wyrafinowany przeciwnik mogący dążyć do odkrycia i wykorzystania luk w oprogramowaniu samolotu, systemach wspomagających lub łańcuchu dostaw, w celu zdobycia informacji wywiadowczych lub sabotowania operacji. Potencjalne ryzyko nie ogranicza się wyłącznie do najnowszych

i najbardziej zaawansowanych systemów: Starsze samoloty, które obecnie jeszcze stanowią większość zapasów US Air Force, są również narażone na ataki ze strony ewoluujących zagrożeń cybernetycznych i muszą zachować czujność.

Aby zarządzać bezpieczeństwem cybernetycznym tych systemów, US Air Force i Departament Obrony USA (DoD ang. Department of Defence, Departament Obrony USA) potrzebują odpowiednich polityk wspierających projekty systemów, które są solidne i odporne na ataki cybernetyczne, projektów organizacyjnych, które są optymalnie ukształtowane, aby wdrożyć te polityki, oraz mechanizmów monitorowania i informacji zwrotnej, które uchwycą prawdziwy stan bezpieczeństwa cybernetycznego (w przeciwieństwie do zwykłej zgodności z obowiązującymi politykami) w całym cyklu eksploatacji systemu broni. Departament Obrony USA zaleca opracowanie modelowej polityki bezpieczeństwa cybernetycznego, do której państwa członkowskie NATO i przedstawiciele branży zbrojeniowej będą mogły się odwoływać przy opracowywaniu własnych polityk krajowych/wewnętrznych. Jedną z kluczowych organizacji powołanych do wsparcia eksploatacji systemów uzbrojenia Sił Powietrznych Stanów Zjednoczonych w pełnym cyklu eksploatacji jest The Air Force Life Cycle Management Center (AFLCMC) Centrum Zarządzania Cyklem Życia Sił Powietrznych z siedzibą w Wright-Patterson AFB. Stanowi ono jedno z sześciu ośrodków podlegających Dowództwu Sił Powietrznych, odpowiedzialnych za zarządzanie cyklem życia systemów uzbrojenia Sił Powietrznych USA od ich powstania do wycofania z eksploatacji. Misją AFLCMC jest wspieranie tych cech uzbrojenia które dzięki technicznej i technologicznej przewadze przechylą szalę zwycięstwa w konfliktach zbrojnych na stronę USA.

AFLCMC zostało zaprojektowane, aby zarządzać systemami uzbrojenia w całym cyklu eksploatacji oraz uprościć i skonsolidować funkcje i procesy personelu w celu ograniczenia redundancji i zwiększenia wydajności. Ponadto struktura operacyjna AFLCMC (rys.1.) zapewnia odpowiednie ramy dla podejmowania decyzji i optymalizacji procesów w całym cyklu życia systemu uzbrojenia. Personel AFLCMC ściśle współpracuje ze swoimi odpowiednikami w pozostałych ośrodkach obejmując nadzorem: systemy i sieci informatyczne; systemy dowodzenia, kontroli, łączności, wywiadu, obserwacji i rozpoznania; uzbrojenia; systemy strategiczne; platformy lotnicze oraz różne systemy specjalistyczne lub wspierające, takie jak np. symulatory i wyposażenie osobiste. AFLCMC realizuje również sprzedaż samolotów i innego sprzętu związanego z obronnością, budując jednocześnie relacje pomocy w zakresie bezpieczeństwa z siłami powietrznymi krajów partnerskich. Zadania te realizuje około dwadzieścia sześć tysięcy specjalistów Sił Powietrznych AFLCMC, pracowników cywilnych i wykonawców centrum z dziewięciu głównych lokalizacji i kilkudziesięciu mniejszych. Dowódca AFLCMC jest odpowiedzialny za organizację, szkolenie i wyposażenie centrum, w tym procesy zarządzania cyklem życia. Każde Biuro Programowe podlega jednemu z 10 Oficerów Wykonawczych Programu (PEO ang. Program Executive Director, Oficer Wykonawczy Programu), którzy są odpowiedzialni za działania w ramach swojego zakresu odpowiedzialności i podlegają Air Force Service Acquisition Executive w Pentagonie (Assistant Secretary of the Air Force for Acquisition). Dyrekcja Wsparcia Bezpieczeństwa i Współpracy Sił Powietrznych nadzoruje realizację misji zagranicznej sprzedaży wojskowej. Dyrekcja Napędów nadzoruje pozyskiwanie silników i wsparcie produktowe. Dyrekcje wsparcia AFLCMC zapewniają bezpośrednie wsparcie programowe, takie jak inżynieria, zarządzanie zamówieniami technicznymi, planowanie rozwoju, kontraktowanie i pomoc w wyborze źródeł dostaw. Dyrekcje wsparcia obejmują: Program Execution; Technical Engineering Services; Financial Management Mission; Logistics Services; Contract Execution; Cyber & Analysis Programs; Program Development & Integration oraz Intelligence.

Centrum Zarządzania Cyklem Życia US Air Force zwróciło się do RAND Project AIR FORCE (PAF) z prośbą o ocenę obecnych przepisów, polityk, organizacji i procesów pod kątem najlepszych praktyk i solidnych zasad cyberbezpieczeństwa oraz o zarekomendowanie kroków w celu poprawy. Badania skupiły się na systemach



***1**. Struktura organizacyjna AFLCMC. Źródło:https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383*

bezpieczeństwa narodowego, dla których Siły Powietrzne mają pewną kontrolę nad projektami, architekturami, protokołami i interfejsami, w przeciwieństwie do komercyjnych, gotowych systemów informatycznych i biznesowych (COTS ang. Commercial Off-The-Shelf – prosto z półki). Misją PAF jest prowadzenie zintegrowanego programu obiektywnych analiz w kwestiach będących przedmiotem trwałego zainteresowania Departamentu Sił Powietrznych. PAF zajmuje się dalekosiężnymi i wzajemnie powiązanymi pytaniami: Jaka będzie rola sił powietrznych i kosmicznych w przyszłym środowisku bezpieczeństwa? Jak należy modernizować siły, aby sprostać zmieniającym się wymaganiom operacyjnym? Jaka powinna być wielkość i charakterystyka pracowników departamentu i jak można ją najskuteczniej rekrutować, wyszkolić i zatrzymać w służbie? Jak należy usprawnić utrzymanie i pozyskiwanie infrastruktury, aby kontrolować koszty?

PAF pierwotnie znany jako Projekt RAND (– nazwa RAND jest skrótem od Research ANd Development (badania i rozwój), został założony w 1946 roku przez generała H. H. "Hap" Arnolda jako sposób na zachowanie znacznych korzyści płynących z cywilnej myśli naukowej, które zostały zademonstrowane podczas II wojny światowej. Od momentu powstania, PAF pozostaje jedynym finansowanym przez Departament Sił Powietrznych centrum badawczo-rozwojowym (FFRDC - Federally Financed Research And Development Center) zajmującym się wyłącznie badaniami i analizami, a nie inżynierią systemów czy laboratoriami naukowymi. Specjalny status FFRDC ułatwia stabilne wsparcie Departamentu Sił Powietrznych przez dłuższy okres czasu, jak również dostęp personelu badawczego do odpowiednich informacji Departamentu i personelu zarządzającego. Zapotrzebowanie Departamentu Sił Powietrznych na wsparcie analityczne ze strony PAF doprowadziło do ustanowienia czterech programów badawczych reprezentujących podstawowe możliwości:

- STRATEGIA I DOKTRYNA dąży do zwiększenia wiedzy i zrozumienia problemów geopolitycznych i innych problemów w środowiskach bezpieczeństwa narodowego, które mają wpływ na operacje Departamentu Sił Powietrznych. PAF wykonuje ekspertyzy w zakresie wielkiej strategii; ewoluujących wyzwań bezpieczeństwa; projekcji siły; operacji ekspedycyjnych; oraz zmieniających się ról sił powietrznych, kosmicznych i cybernetycznych w obecnych i przyszłych operacjach.
- MODERNIZACJA I ROZWÓJ SIŁ LĄDOWYCH identyfikuje i ocenia sposoby, w jakie postęp technologiczny i nowe koncepcje operacyjne mogą poprawić zdolność Departamentu Sił Powietrznych do zaspokojenia szeregu przyszłych wymagań operacyjnych. Badania te obejmują ocenę wykonalności technologii, wydajności, kosztów i ryzyka. PAF ocenia główne komponenty sił powietrznych, kosmicznych i cybernetycznych potrzebne w przyszłości oraz systemy i infrastrukturę wspierające ich działanie. Obszary specjalizacji obejmują wywiad, nadzór, rozpoznanie, mobilność, uderzenie dalekiego zasięgu, bojowe siły powietrzne, dowodzenie i kontrolę, przestrzeń kosmiczną, cybernetyczną i nuklearną.
- RESOURCE MANAGEMENT analizuje polityki i praktyki w ramach trzech tematów: (1) odporności instalacji DAF (ang. Detect-A-Fire, instalacja wykrywania pożaru), aktywów i informacji, (2) skutecznej i efektywnej alokacji zasobów oraz, (3) zdrowia bazy przemysłowej i technologicznej obrony. Celem badań prowadzonych w ramach programu jest maksymalizacja skuteczności i efektywności operacji w środowisku o ograniczonych zasobach.

WORKFORCE, DEVELOPMENT, AND HEALTH (dawniej Manpower, Personnel, and Training) bada wielkość i skład personelu Departamentu Sił Powietrznych oraz zajmuje się najlepszymi sposobami definiowania, podtrzymywania, odnawiania, dostarczania i koordynowania krytycznych zdolności roboczych. PAF rozważa również rozwój personelu, taki jak szkolenia, możliwości zatrudnienia i awansu zawodowego, a także analizuje zdrowie fizyczne i psychiczne pracowników. Badania PAF obejmują całą siłę roboczą: aktywną służbę, gwardię, rezerwę, personel cywilny i wykonawczy. PAF prowadzi również szeroko zakrojone badania na tematy, które dotyczą wszystkich czterech programów, a także regularnie odpowiada na prośby Sił Powietrznych o pomoc w rozwiązaniu pilnych problemów.

Spostrzeżenia dotyczące zarządzania bezpieczeństwem cybernetycznym.

Eksperci PAF wyszli z założenia, że pożądanymi rezultatami zarządzania bezpieczeństwem cybernetycznym jest (1) ograniczenie ilości informacji krytycznych, które może uzyskać przeciwnik w wyniku udanej eksfiltracji oraz (2) utrzymanie akceptowalnego poziomu funkcjonalności operacyjnej nawet w przypadku ataku. Wyniki te muszą być osiągane w sposób ciągły przez cały cykl życia systemu wojskowego, od badań i rozwoju do utylizacji. Wszystkie etapy są ważne, ale etapy rozwoju i utrzymania są szczególnie krytyczne: pierwszy z nich wynika z podejmowania decyzji projektowych, które mogą ograniczyć możliwości w przyszłości, a drugi z faktu, że większość systemów pozostaje w stanie utrzymania przez większość cyklu życia. Biorąc pod uwagę te cele w zakresie bezpieczeństwa cybernetycznego, przegląd literatury

ujawnia dwie obserwacje dotyczące projektu organizacyjnego i informacji zwrotnej w celu osiągnięcia tych celów w zakresie bezpieczeństwa cybernetycznego.

Projekt organizacyjny powinien być elastyczny i zdecentralizowany. Środowisko cyberbezpieczeństwa jest z natury dynamiczne i złożone. Literatura sugeruje, że dobrze zarządzane organizacje radzą sobie z takim środowiskiem wybierając projekty organizacyjne, które faworyzują rozwiązania uzyskane poprzez zdecentralizowaną koordynację i współpracę pracowników nad rozwiązaniami zalecanymi przez standardowe i sformalizowane kontrole. Informacje zwrotne oparte na wynikach są bardziej wartościowe niż informacje zwrotne oparte na zgodności. Organizacje mają tendencję do skupiania się na łatwo obserwowalnych wskaźnikach, takich jak zgodność z politykami i dyrektywami, aby wskazać swój poziom bezpieczeństwa cybernetycznego. Jednak zgodność sama w sobie nie odzwierciedla rzeczywistego stanu bezpieczeństwa cybernetycznego, zwłaszcza w złożonych i szybko zmieniających się środowiskach zagrożeń. Organizacje powinny raczej skupić się na tym, czy ich polityka i praktyki osiągają pożądane rezultaty (np. zapewnienie misji w obliczu adaptacyjnych cyberataków) i powinny być gotowe do dostosowania się w razie potrzeby.

Obecne braki i ich implikacje

Porównanie tych zasad zarządzania ze szczegółowym przeglądem przepisów i polityk regulujących cyberbezpieczeństwo w US Air Force ujawnia szereg luk. Obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości środowiska bezpieczeństwa cybernetycznego. Departament Obrony USA dąży do standaryzacji bezpieczeństwa cybernetycznego poprzez zastosowanie kontroli bezpieczeństwa Narodowego Instytutu Standardów i Technologii (NIST) do wszystkich systemów, w tym systemów uzbrojenia. Kontrole te mają na celu złagodzenie problemów bezpieczeństwa w projektach, które Siły Powietrzne dziedziczą, takich jak systemy COTS. Z kolei systemy uzbrojenia dają projektantom możliwość budowania systemów, które są bardziej bezpieczne z natury. Solidna inżynieria bezpieczeństwa systemu na wczesnym etapie projektowania systemu broni byłaby bardziej skuteczna niż kontrole bezpieczeństwa, które są stosowane jako nakładki na projekty stworzone bez cyberbezpieczeństwa jako integralnego priorytetu. Bezpieczeństwo cybernetyczne opiera się na danych wywiadowczych, zagrożeniach i zarządzaniu ryzykiem, które stanowi integralną część całego cyklu życia systemów. Wszystkie dane i systemy muszą mieć przez cały czas ustalonego właściciela. Funkcje, systemu i infrastruktura o znaczeniu krytycznym są identyfikowane w ramach procesów zarządzania ryzykiem. Do ochrony systemów krytycznych stosuje się podejście "security by design" w połączeniu z zasadami "Defence in depth". Redundancja systemów krytycznych jest traktowana jako czynnik zwiększający bezpieczeństwo systemu. Dane i informacje są chronione podczas przechowywania i przekazywania, zgodnie z ich wrażliwościami. Zarządzanie całym łańcuchem dostaw oprogramowania/sprzętu komputerowego stanowi część zarządzania bezpieczeństwem cybernetycznym lotnictwa. Oprogramowanie i sprzęt wykorzystywany w krytycznych funkcjach lotnictwa muszą spełniać wymogi w zakresie bezpieczeństwa cybernetycznego przez cały cykl życia bojowych systemów lotniczych. Ochrona fizyczna (w tym ochrona personelu) jest częścią zarządzania cyberbezpieczeństwem w lotnictwie. Zadaniem ochrony fizycznej jest zabezpieczenie ludzi, infrastruktury, obiektów, sprzętu, materiałów i dokumentów przed bezprawną ingerencją oraz ochrona krytycznych systemów lotniczych przed nieuprawnionym dostępem fizycznym. Ochrona fizyczna przyczynia się do zarządzania ryzykiem poprzez identyfikację podmiotów stanowiących zagrożenie i/lub prawdopodobieństwo ataków na krytyczną infrastrukturę lotnictwa wojskowego. Ochrona informacji, komunikacji i technologii (ICT) jest częścią zarządzania cyberbezpieczeństwem lotnictwa, określa i wdraża logiczne środki bezpieczeństwa, a także przyczynia się do zarządzania incydentami cybernetycznymi, odzyskiwania danych i ciągłości działania w procesach zarządzania incydentami cybernetycznymi, odzyskiwania danych i ciągłości działania. Bezpieczeństwo teleinformatyczne przyczynia się do zarządzania ryzykiem poprzez identyfikację podatności, obszarów i kierunków ataku oraz monitorowanie zmian w krajobrazie zagrożeń dla bezpieczeństwa cybernetycznego. Zarządzanie incydentami i ciągłość funkcji krytycznych są głównymi czynnikami w procesach zarządzania incydentami. Nieodłącznym procesem jest testowanie planów zarządzania kryzysowego i odzyskiwania danych, które stanowi integralną część zarządzania incydentami.

Wdrażanie bezpieczeństwa cybernetycznego nie jest stale aktywne przez cały cykl życia systemu wojskowego. Zwrócenie uwagi na bezpieczeństwo cybernetyczne jest zazwyczaj wywoływane przez wydarzenia związane z pozyskiwaniem uzbrojenia, które najczęściej mają miejsce podczas zamówień publicznych. W rezultacie polityka nie obejmuje pełnego zakresu kwestii związanych z bezpieczeństwem cybernetycznym, które mają wpływ na system w całym jego cyklu życia. Ten brak ma kilka istotnych konsekwencji. Po pierwsze, programowe czynniki wyzwalające w zakresie bezpieczeństwa cybernetycznego pojawiają się na późnym etapie procesu projektowania i w

związku z tym mają niewielki wpływ na kluczowe decyzje projektowe, które mają wpływ na bezpieczeństwo cybernetyczne. Po drugie, systemom w programach znajdujących się poza fazą zamówień publicznych (tj. w fazie podtrzymywania lub likwidacji) poświęca się mniej uwagi niż systemom w fazie zamówień publicznych. Jak wspomniano powyżej, powoduje to niedocenianie większości systemów US Air Force, które są w fazie konserwacji. Po trzecie, ta struktura polityki ma tendencję do faworyzowania ocen podatności (przeważających w fazie projektowania) nad ocenami wpływu misji i zagrożeń (które mają wpływ na cały cykl życia). Wreszcie, zarządzanie, nadzór i budżetowanie w ramach Departamentu Obrony Stanów Zjednoczonych są silnie ustrukturyzowane wokół programów, podczas gdy podatności w zakresie bezpieczeństwa cybernetycznego przekraczają granice programów. Powoduje to rozbieżność między wyzwaniami w zakresie bezpieczeństwa cybernetycznego w poszczególnych systemach a sposobem zarządzania nimi.

Monitorowanie i informacje zwrotne dotyczące bezpieczeństwa cybernetycznego są niepełne, nieskoordynowane i niewystarczające do skutecznego podejmowania decyzji lub odpowiedzialności. Obecne informacje zwrotne nie obejmują wszystkich systemów, nie badają konsekwencji braków w zakresie bezpieczeństwa cybernetycznego i nie są przekazywane w formie umożliwiającej podejmowanie skutecznych decyzji. Brak kompleksowych, zorientowanych na program lub system informacji zwrotnych na temat bezpieczeństwa cybernetycznego oraz wpływu bezpieczeństwa cybernetycznego na misje operacyjne kontrastuje z dużą ilością informacji zwrotnych na temat kosztów i harmonogramu. Ta nierównowaga stwarza strukturę motywacyjną dla kierowników programów i dyrektorów wykonawczych programów, którzy przedkładają koszty i harmonogram nad wyniki w zakresie bezpieczeństwa cybernetycznego. Te braki w informacjach zwrotnych dotyczących bezpieczeństwa cybernetycznego dodatkowo ograniczają indywidualną odpowiedzialność.

Zalecenia mające na celu usunięcie niedociągnięć

Żadne proste rozwiązanie nie skoryguje wszystkich powyższych braków, z których wiele jest strukturalnie zakorzenionych w Departamencie Obrony USA. Niektóre wynikają z dobrze pomyślanych wymogów ustawowych i polityk Departamentu Obrony, które niełatwo zmienić. Jednakże, w ramach tych ograniczeń, istnieją kroki, które Siły Powietrzne mogą podjąć w celu wzmocnienia bezpieczeństwa cybernetycznego systemów uzbrojenia:

- Zdefiniowanie celów cyberbezpieczeństwa dla systemów wojskowych w Siłach Powietrznych wokół pożądanych wyników, pozostając jednocześnie w zgodzie z wytycznymi Departamentu Obrony. Cel roboczy stanowi utrzymanie wpływu wykorzystania cybernetycznego i ofensywnych operacji cybernetycznych przeciwnika na akceptowalnym poziomie, zgodnie ze standardowym procesem oceny ryzyka dla zapewnienia misji.
- Przeformułowanie ról i obowiązków funkcjonalnych w zakresie oceny ryzyka związanego z bezpieczeństwem cybernetycznym w oparciu o równowagę między podatnością systemu, zagrożeniem i wpływem na misję operacyjną, a także nadać urzędnikowi zatwierdzającemu uprawnienia do integracji i rozstrzygania między zainteresowanymi stronami. Na przykład społeczność zarządzająca cyklem życia (w szczególności kierownik programu) byłaby odpowiedzialna za oceny podatności programu i systemu, społeczności wywiadowcze i kontrwywiadowcze byłyby odpowiedzialne za oceny zagrożeń, a właściciel misji (np. główny integrator funkcji podstawowych, główne dowództwo) byłby odpowiedzialny za oceny zapewnienia misji operacyjnej. Urzędnik zatwierdzający integruje i równoważy te punkty widzenia w oparciu o akceptowalny poziom ryzyka cyberbezpieczeństwa.
- Przydzielenie każdemu urzędnikowi zatwierdzającemu portfela systemów i zapewnienie, że wszystkie systemy wyraźnie podlegają jakiemuś urzędnikowi zatwierdzającemu przez cały cykl życia.
- Zachęcanie biur programowych US Air Force do uzupełnienia wymaganych kontroli bezpieczeństwa DoD (które koncentrują się na likwidowaniu słabych punktów) o bardziej kompleksowe środki bezpieczeństwa cybernetycznego, w tym solidną inżynierię bezpieczeństwa systemu (która koncentruje się na zapewnieniu solidności i odporności systemu w obliczu udanych ataków).
- Wspieranie innowacji i adaptacji w zakresie bezpieczeństwa cybernetycznego poprzez decentralizację, w ramach każdej nowej polityki US Air Force, sposobu wdrażania inżynierii bezpieczeństwa systemu w ramach poszczególnych programów.
- Ocenę kompromisów między ryzykiem związanym z bezpieczeństwem cybernetycznym a korzyściami funkcjonalnymi związanymi z łączeniem systemów wojskowych w cyberprzestrzeni. Celem jest odwrócenie domyślnej kultury łączenia systemów, gdy tylko jest to możliwe, i zmniejszyłoby złożoność bezpieczeństwa cybernetycznego.
- Stworzenie grupy ekspertów w dziedzinie bezpieczeństwa cybernetycznego, którzy mogą

być w razie potrzeby łączeni w ramach społeczności cyklu życia, udostępniając zasoby małym programom i programom w fazie podtrzymywania.

- Ustanowienie priorytetów dla przedsiębiorstw w zakresie oceny i rozwiązywania problemów bezpieczeństwa cybernetycznego w starszych systemach.
- Zlikwidowanie luk w informacjach zwrotnych i zwiększenie widoczności cyberbezpieczeństwa poprzez sporządzanie regularnej, ciągłej oceny podsumowującej stan cyberbezpieczeństwa dla każdego programu w US Air Force. Pociągnąć kierowników programów do odpowiedzialności za reakcję na problemy.
- Stworzenie czerwonych zespołów ds. cyberbezpieczeństwa, które są dedykowane do zarządzania nabyciem/cyklem życia w US Air Force.
- Pociągnięcie osób do odpowiedzialności za umyślne naruszenie zasad cyberbezpieczeństwa.
- Opracowanie danych dotyczących zagrożeń misji w celu wsparcia kierowników programów i urzędników zatwierdzających w ocenie akceptowalnego ryzyka dla misji spowodowanego brakami w zakresie bezpieczeństwa cybernetycznego w systemach i programach.

Należy zdawać sobie sprawę, iż zalecenia te, nawet jeśli zostaną w pełni wdrożone, nie rozwiążą całkowicie problemów związanych z bezpieczeństwem cybernetycznym. Co więcej, niektóre z tych polityk wymagałyby dodatkowych zasobów i odpowiednio wykwalifikowanej siły roboczej do realizacji obowiązków - zobowiązań, które są trudne do podjęcia w ograniczonym środowisku fiskalnym. Faktem jest, że nie ma szybkich ani łatwych rozwiązań pozwalających osiągnąć światowej klasy bezpieczeństwo cybernetyczne. Jednak przyjmując te zalecenia, Siły Powietrzne zrobiłyby duży krok w kierunku skuteczniejszego zabezpieczenia cybernetycznego swoich systemów wojskowych w całym cyklu ich życia. Kultura bezpieczeństwa cybernetycznego jest bardzo ważnym elementem polityki bezpieczeństwa. Opracowany dla jej wdrażania plan edukacji, świadomości, szkoleń i ćwiczeń stanowi integralną część zarządzania bezpieczeństwem cybernetycznym systemów uzbrojenia sił powietrznych. Kultura bezpieczeństwa cybernetycznego jest w pełni skoordynowana z istniejącymi kulturami bezpieczeństwa i ochrony, wspierają ją solidne wewnętrzne i w miarę możliwości, zewnętrzne praktyki wymiany informacji.

Główne wnioski

Audyty cyberbezpieczeństwa wykazują iż obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości środowiska bezpieczeństwa cybernetycznego.

- Wdrożenie bezpieczeństwa cybernetycznego nie jest stale utrzymywane na odpowiednim poziomie przez cały cykl życia systemu wojskowego.
- Kontrola i odpowiedzialność za bezpieczeństwo cybernetyczne systemów wojskowych jest rozłożona na wiele organizacji i słabo zintegrowana.
- Monitorowanie i informacje zwrotne dotyczące cyberbezpieczeństwa są niekompletne, nieskoordynowane i niewystarczające do skutecznego podejmowania decyzji lub odpowiedzialności struktur i osób funkcyjnych.

Modelowa polityka bezpieczeństwa cybernetycznego ma służyć jako przewodnik pomagający państwom i ich siłom zbrojnym skupić zasoby i działania mające na celu osiągnięcie systemowego podejścia do cyberbezpieczeństwa w US Air Force, w tym do obecnych i systemy dotychczasowe. Ostatecznym celem jest, aby państwa oraz zainteresowane strony były w stanie opracować podejście typu system systemów (system-of--systems), które umożliwi ochronę przed zagrożeniami cybernetycznymi oraz reagowanie na incydenty cybernetyczne i usuwanie ich skutków w odpowiednim czasie, a tym samym odporność na nowe zagrożenia bez znaczących zakłóceń.

Główne wyniki, jakich oczekuje się po wdrożeniu polityki bezpieczeństwa cybernetycznego to określenie ram dla dalszego rozwoju i wdrażania bezpieczeństwa cybernetycznego w Siłach Powietrznych. Będzie to realizowane dzięki publikowaniu i rozpowszechnianiu polityki bezpieczeństwa wśród właściwych zainteresowanych struktur i poddawaniu jej okresowym przeglądom.◀

Materiały źródłowe

[1] website belongs to an official U.S. Department of Defense organization in the United States.
[2] https://www.afsbirsttr.af.mil/About/Cybersecurity-and-the-Blue-Cyber-Education-Series/
[3] Official websites use .mil ., An official website of the United States government
[4] https://hii.com/wp-content/uploads/2023/03/HII-Game--Changer-9.1.22.pd
[5] https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383
[6] https://nap.nationalacademies.org/read/25393/chapter/1
[7] https://www.aflcmc.af.mil/WELCOME/Organizations/
[8] https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf

Cyberbezpieczeństwo a rewolucja cyfrowa (na przykładzie domeny cywilnej i wojskowej)

Cybersecurity and the digital revolution (on the example of the civil and military domain)

Lech Majewski

gen. broni pil. w stanie spoczynku

wiceprezes SSLW RP,
przewodniczący KSLiTK przy SITKRP

Streszczenie: Pojawienie się nowych technologii cyfrowych stwarza nowe możliwości rozwoju i budowania zdolności materialnych, ale i duże zmiany w życiu społecznym, w wymiarze prawnym, czy w zakresie etyki. Śmiało można stwierdzić, że ten kto szybciej i lepiej wykorzysta możliwości, jakie daje sztuczna inteligencja, kosmos i cyberprzestrzeń - będzie kształtował przyszłość świata, tworzył nową cywilizację, zmieniał podstawy jej funkcjonowania. Ten proces już się rozpoczął. Największe potęgi militarne na świecie na pierwszym miejscu stawiają cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpracę z pilotowanymi samolotami lub załogowymi okrętami, sztuczną inteligencją oraz wykorzystaniu przestrzeni kosmicznej i cyberprzestrzeni. Należy tu podkreślić, ze podjęte działania pozwalają prowadzić działania bojowe w czasie rzeczywistym. Powstaje świat zdeformowany poznawczo w którym trudno jest ocenić obiektywnie zaistniałe sytuacje. Bowiem inaczej oceniają sytuację Stany Zjednoczone, a inaczej Europa, inaczej Chiny i Rosja. System polityczny Chin pozwala łatwiej i szybciej opanowywać domenę cyber. Chiny sukcesywnie uzyskują przewagę technologiczną, opanowują nowe technologie, nie mają przy tym cywilizacyjno-kulturowych obiekcji.

Słowa kluczowe: Cyberprzestrzeń; Rewolucja cyfrowa; Przestrzeń kosmiczna; Lotnictwo

Abstract: The emergence of new digital technologies creates new opportunities for development and building material capabilities, but also major changes in social life, in the legal dimension, or in the field of ethics. It can be safely said that the one who makes better and faster use of the opportunities offered by artificial intelligence, space and cyberspace will shape the future of the world, create a new civilization, change the basis of its functioning. This process has already started. The largest military powers in the world put digital technologies, autonomous and unmanned systems in the first place - their cooperation with piloted aircraft or manned ships, artificial intelligence and the use of space and cyberspace. It should be emphasized here that the actions taken allow to carry out combat operations in real time. A cognitively deformed world is created in which it is difficult to objectively assess the existing situations. Because the United States assesses the situation differently than Europe, China and Russia. China's political system makes it easier and faster to control the cyber domain. China successively gains a technological advantage, masters new technologies, and does not have any civilizational and cultural objections.

Keywords: *Cyberspace; digital revolution; Outer space; Aircraft*

Żyjemy w okresie rewolucyjnych zmian technologicznych, w okresie czwartej rewolucji przemysłowej, która zachodzi bardzo szybko. Rewolucja cyfrowa wpływa na nasze codzienne życie, determinuje rozwój państwa i jego miejsce w strukturze przyszłego świata. Staje się rdzeniem postępu, a w Siłach Zbrojnych jest zapowiedzią nowego typu wojny.

Siłą napędową czwartej rewolucji przemysłowej jest kombinacja nowoczesnych komputerów o wysokiej mocy obliczeniowej, robotów, zestawów autonomicznych i rozszerzonych technologii informacyjnych, ale i lepsze poznanie i wykorzystanie ludzkiego genomu.

To właśnie wzajemne połączenie różnych urządzeń, dostęp do jak największej ilości informacji, wsparcie technologiczne jak i decentralizacja decyzji może przekładać się na autonomiczność decyzji, szybszą komunikację i efektywną współpracę. Jednocześnie nowa sytuacja skutkuje potrzebą szybkiego identyfikowania problemów, z którymi wcześniej nie mieliśmy do czynienia.

Kluczową rolę odgrywa tu analityka Big Data i algorytmy sztucznej inteligencji. Inteligentne systemy dysponują wszechstronną wiedzą i zdolnościami poznawczymi, które potrafią samodzielnie wykonywać zadania.

Oprócz istniejących domen prowadzenia działań wojennych: lądowej, morskiej, powietrznej, zaczyna dominować domena kosmiczna oraz cyberprzestrzeń (cyfrowa) .

W lipcu 2016 roku, podczas Szczytu NATO w Warszawie, uznano przestrzeń cybernetyczną za kolejną domenę (wtedy czwartą), w której mogą być prowadzone działania operacyjne. Jed-

nocześnie członkowie NATO podkreślili, że dołożą wszelkich starań, aby nowa domena operacyjna była broniona w taki sam sposób, w jaki Sojusz chroni swoje operacje w wymiarze lądowym, morskim i powietrznym. W tym celu przyjęto 7 zobowiązań znanych jako Cyber Defence Pledge, które sojusznicy zgodzili się rozwijać i wzmacniać. Jednocześnie uzgodniono, że stan wdrażania w/w zobowiązań będzie monitorowany i sprawdzany przez NATO w odstępach rocznych.

Cyberprzestrzeń już w czasie pokoju poddawana jest ciągłym atakom. Systematycznie atakowana jest infrastruktura krytyczna, systemy łączności, przestrzeń informacyjna.

Na naszych oczach kształtują się dwa światy cyfrowe: Chiński i proamerykański. Trwa wielka rewolucja i rywalizacja. Polska, ale i inne państwa naszego układu, bardzo często są przedmiotem ataków cybernetycznych ze strony różnych państw, przede wszystkim ze strony Federacji Rosyjskiej. W takiej sytuacji, a szczególnie w kontekście wojny w Ukrainie nie powinniśmy pozwolić aby pozostać w tyle w tym zakresie.

Wszystko wskazuje na to że najważniejsza wojna XXI wieku rozegra się w świecie wirtualnym, w cyberprzestrzeni - w tym kierunku największe potęgi militarne prowadzą intensywne przygotowania i działania. Tworzą się nowe strategie prowadzenia wojen. Na pewno bezpieczeństwo Polski jest bardziej zagrożone teraz, niż na przykład 10 lat temu.

Coraz częściej mówimy o wojnie bezkontaktowej o autonomicznych środkach prowadzenia walki, robotach bojowych, nowych systemach broni elektromagnetycznej, laserowej, plazmowej i mikrofalowej, o bojowych egzoszkieletach, implantach uodporniających żołnierzy na stres.

Największe potęgi militarne na świecie na pierwszym miejscu stawiają cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpracę z pilotowanymi samolotami lub załogowymi okrętami, sztuczną inteligencją oraz wykorzystaniu przestrzeni kosmicznej i cyberprzestrzeni. Należy podkreślić, ze podjęte działania pozwalają prowadzić działania bojowe w czasie rzeczywistym.

Efektem tego jest zwiększenie znaczenia działań bezkontaktowych, w których walczące strony są poza zasięgiem bezpośredniej obserwacji, gdzie brak jest rubieży styczności bojowej wojsk, gdzie uderzenie na potencjalnego przeciwnika może zostać wykonane ze wszystkich kierunków, ze wszystkich domen prowadzenia działań operacyjnych.

Pentagon przewiduje, że w nadchodzącej dekadzie autonomiczne systemy staną się jednym z głównych środków walki. Obecnie trwające prace nad programem tzw. przyszłych systemów bojowych (FCS – Future Combat Systems), których wartość jest oceniana na ponad 120 mld dolarów. Jest to największy kontrakt w historii USA.

W Stanach Zjednoczonych coraz wyraźniej mówi się, ale i realizuje następujące filary modernizacji Sił Zbrojnych:

1. Sieciowy (sieciocentryczny) system kierowania i dowodzenia. Idea połączenia wszystkiego ze wszystkim oraz tworzenie rzeczywistości rozszerzonej, pozwalającej na projektowanie dodatkowych informacji na obraz świata rzeczywistego. Poligonem doświadczalnym są oczywiście SP.
2. Systemy autonomiczne współpracujące z ludźmi, wdrażane we wszystkich Rodzajach Sił Zbrojnych na masową skalę.
3. Sztuczna inteligencja – klucz do danych, a dane są dziś polem walki.

Nie mówi się o czołgach, samolotach, rakietach, okrętach, a nawet o satelitach – mówi się o sieciach, łączności, danych i potencjale technologii AI (artficial intelligence), który automatyzuje procesy, przewiduje przyszłe zdarzenia, szacuje ryzyka i profilaktyktykę. Nie megatony a megabity.

Wartość globalnego rynku sztucznej inteligencji w 2022 roku osiągnęła wartość około 450 mld. dol. Do 2030 roku wartość sektora AI wzrośnie do 1,3 bln dolarów oraz zwiększy wartość światowej gospodarki o prawie 16 bilionów dolarów. Do roku 2022 dzięki nowym technologiom powstało na świecie 133 mln. miejsc pracy.

Tylko w 2019 roku światowe wydatki na AI osiągnęły prawie 40 mld. dol. 44% więcej niż rok wcześniej (2/3 USA; 5,5% Europa).

Szacuje się, że cyberataki w 2021 roku kosztowały nawet 11,4 mln. $ na minutę! Jedna złotówka zainwestowana w przemysł kosmiczny zwraca się czterokrotnie.

W Polsce w ciągu najbliższych pięciu lat zapotrzebowanie na specjalistów zajmujących się sztuczną inteligencją sięgnie 200 tys. osób.

Wiele państw na czele z Rosją prowadzi intensywne działania cybernetyczne łamiąc prawo międzynarodowe, ingerując w ich politykę wewnętrzną. Używając siły militarnej przeciwko sąsiadom: Gruzji i Ukrainie, ale i odpowiada także za agresywne działania wobec państw NATO. Wszystkie te działania wpływają również na wewnętrzne procesy polityczne państw.

W marcu 2021 roku prezydent Biden powiedział, że prezydent Rosji jest „zabójcą" i że zapłaci za ingerencję w wybory w USA.

Polska wydaje setki miliardów na nowe uzbrojenie.

Jednak czy decydenci zdają sobie sprawę, że droga do przyszłości Sił Zbrojnych, do skutecznej obrony państwa, to sztuczna inteligencja, systemy autonomiczne i sieciocentryczność, że tu jest potencjał, a nie w czołgach czy rakietach, że żaden, nawet najnowocześniejszy środek współczesnego pola walki nie ma żadnego znaczenia, jeśli nie będzie wpięty w odporną na zakłócenia i bardzo przepustową sieć informatyczną.

Gwałtowny rozwój technologii informatycznych spowodował jej zastosowanie do działań w cyberprzestrzeni. Szczególnie w celu uszkodzenia infrastruktury krytycznej (banki, energetyka czy obiekty przemysłowe i wojskowe np. systemy kierowania i dowodzenia).

Robotyzacja w przemyśle, ale i na polu walki w krótkim okresie doprowadzi do ich pełnej autonomii podczas realizacji stawianych zadań.

Australia: armia stawia na roboty i

nowe podejście do robotów.

Australijczycy nie tylko widzą rosnące zagrożenia, ale podejmują konkretne działania. Zaczynają prowadzić szeroki program testów i badań dotyczących przełomowych technologii w tym autonomicznych robotów lądowych. Program bazuje na szerokiej współpracy wojska, przemysłu i nauki, ale i oczywiście ze Stanami Zjednoczonymi.

W Australii nie mówi się o samych robotach, ale już się je eksploatuje, testuje lub rozwija programy rozwojowe.

TURCJA: planuje stworzenie lotniskowca dla 30-50 dronów bojowych (wcześniej planowane dla F-35 – zakup S-400 zmienił plany).

Satelity Elona Muska są niezbędne dla ukraińskiej armii i ludności cywilnej - pomagają w ustalaniu rosyjskich pozycji, umożliwiają kontakt z bliskimi, a przemówienia prezydenta Wołodymyra Zełenskiego mogą być transmitowane na całym świecie.

Dzięki systemowi od SpaceX Kremlowi nie udało się odciąć Ukrainy od świata zewnętrznego, a plany Kremla okazały się nierealne.

Wojna w Ukrainie bardzo wyraźnie pokazuje, że coraz większy dostęp do sztucznej inteligencji, kosmosu i najnowszych technologii powoduje, ze prawda staje się pierwszą ofiarą zaistniałej sytuacji.

Na przykładzie ostatnich zdarzeń politycznych, sytuacji w masmediach oraz wewnętrznej sytuacji w Ukrainie coraz częściej mówimy o „mgle wojny". Powstaje przekazywana informacja na podstawie której trudno jest określić dynamikę zdarzeń w zaistniałej sytuacji np. sytuacji i strat na froncie ukraińskim.

Ta nowa infosfera (nie zawsze doceniana) przyczyniła się miedzy innymi do tego, ze NATO, UE, ale i Stany Zjednoczone nie były zdolne ocenić sytuacji na wschodzie i powstrzymać agresywne działania Rosji. Dominacja mediów społecznościowych w systemie demokratycznym stała się bezsprzeczna i trudna do opanowania. Setki tysięcy pośredników nie produkcyjnych w strukturach państwa staje się dużą bolączka zachodu, często kształtuje i spowalnia rozwój.

W aspekcie dominacji cyfrowej, szybkim rozwojem nowych sposobów komunikacji w tym mediów społecznościowych dużym problemem staje się legitymizacja władzy. Media społecznościowe wydatnie mogą się przyczynić do zakłócenia sytuacji w państwie, mogą stać się elementem strategii biznesowej. Bardzo wyraźnie zmniejsza się rola autorytetów. Korzystanie z Internetu bez ograniczeń i nadzoru może uzależniać i powodować problemy psychologiczne szczególnie wśród osób młodych.

Dlatego ważnym aspektem operowania w cyberprzestrzeni jest posiadanie umiejętności monitorowania informacji ze szczególnym uwzględnieniem dynamiki rozwoju wirtualnych społeczności. Internet to doskonały środek dla fałszywych liderów, kreujących się jako osoby kompetentne, co w dobie post-prawdy nie jest w żaden sposób weryfikowane. Tego typu mechanizmy społeczne są często wykorzystywane przez organizacje terrorystyczne i przestępcze, ale i instytucje polityczne i państwowe.

Jeżeli porównamy potencjał militarny i ekonomiczny UE, NATO i USA do potencjału Rosji to różnice są porażające, a jednak Rosja zaatakowała….

Powstał świat zdeformowany poznawczo w którym trudno jest ocenić obiektywnie zaistniałe sytuacje. Inna jest ocena sytuacji przez USA, Europę, Chiny, nie mówiąc już o Rosji. Zachód na czele z Francją czy Niemcami często obawia się możliwości dominacji USA.

W innej sytuacji są Chiny. Ich system polityczny pozwala im łatwiej i szybciej opanowywać domenę cyber. Chiny sukcesywnie uzyskują przewagę technologiczną, opanowują nowe technologie, nie mają cywilizacyjno - kulturowych obiekcji.

W świecie demokratycznym, powstanie wielkich światowych korporacji cyfrowych przy braku odpowiedniej reakcji świata politycznego powoduje niszczenie małego biznesu oraz klasy średniej , generuje napięcia społeczne. Biznes z Doliny Krzemowej, generuje ogromne pieniądze i uzyskuje przewagę nad polityką.

Powstaje węzeł gordyjski: jeżeli podzielimy potężne zachodnie koncerny – nie będzie możliwości konkurencji z potężnymi Chińskimi.

W Chinach kapitał cyfrowy nie ma przewagi nad polityką, nad rządem.

Dyskusja i konflikt - swoboda wyrażania poglądów są normalnością w demokratycznych społeczeństwach. W Internecie istnieją narzędzia, które umożliwiają monitorowanie i administrowanie tego typu procesami.

Największym zagrożeniem wydają się być zamknięte grupy kontrolowane przez liderów, których potencjału i aspiracji nie da się zweryfikować w rzeczywistym świecie. Wykorzystując prosty schemat, trójkąt oprawca -ofiara - wybawca można zilustrować relacje zarówno w radykalnych organizacjach jak i w życiu codziennym. Efektem jest proces sprawiający gwałtowną brutalizację stosunków międzyludzkich.

Prowadzą do niego trzy główne czynniki: brak autorytetów, pogorszenie się podstawowych warunków życia (co często prowadzi do stresu i ostatecznie paniki) oraz funkcjonowanie silnych grup nacisku wpływających na bezbronną ofiarę.

W zaistniałej sytuacji, biorąc pod uwagę powstające zagrożenia istnieje pilna potrzeba budowy nowej kategorii polityków, dobrze wykształconych i rozumiejących rzeczywistość, umiejących podjąć stosowne decyzje i to zmienić.

Pandemia Covid przyspieszyła rozwój nowych technologii, sztucznej inteligencji, zmieniła system komunikacji społecznej. Rozwinęła pracę zdalną oraz wirtualne uczenie się na kursach online, zdalne internetowe zakupy, ale i skłonności depresyjne szerokiej grupy społeczeństwa. Zdaniem ekspertów pandemia przyśpieszyła rewolucję cyfrową o wiele lat.

Na naszych oczach domena cyber używana do dezinformacji stała się potężną bronią. Dobrym przykładem jest tutaj Ukraina.

Co by było gdyby Rosja w Ukrainie od początku zaczęła atakować infrastrukturę krytyczną? Rosjanie stworzyli sobie fałszywy obraz Ukrainy. Nie traktowali Ukrainy jako państwa obcego. Sądzili, że Ukraińcy popierają Rosję.

Posiadali zniekształcony obraz sytuacji w Ukrainie. Przeoczyli między innymi Majdan, który wszystko zmienił.
Na początku chcieli przejąć państwo nie zniszczone, mieli poczucie przewagi – na szczęście fałszywe.

W trudnej sytuacji Ukraina pokazała ogromną siłę woli, ogromną kreatywność rządu, ale i normalnych ludzi, wielką wolę walki o wolność i demokrację o przynależność do świata zachodniego.

Proces ograniczania szkód jakie niosą ze sobą barbarzyńskie ataki rosyjskie rozpoczęli już na poziomie budowania infrastruktury informatycznej.
Dobrze zaprojektowali sieć komputerową która funkcjonuje nawet w przypadku zainfekowania poszczególnych terminali. Sieć rozproszona okazała się bardzo odporna na ataki hakerskie, oczywiście jeżeli tylko cyberprzestępcy nie zlokalizują kluczowych urządzeń odpowiedzialnych za przekierowywanie większości ruchu.

Okazało się, że ważnym środkiem podnoszącym bezpieczeństwo infrastruktury jest nadmiarowość komponentów sieciowych – pozwala to na duplikację kanałów przekazu i utrzymanie podstawowych funkcji nawet w przypadku zniszczenia części z nich.

Na poziomie infrastruktury zagwarantowali również właściwe serwisowanie, która zawsze wiąże się z warunkiem doboru zaufanych i zweryfikowanych podwykonawców – co szczególnie w Ukrainie nie było proste.

Do dzisiaj tylko 77 państwa wypracowały własne cyber-strategie, tylko dwadzieścia ma swoje, specjalne dowództwa, a jedynie 17 z nich jest zdolne do przeprowadzania cyberataków.

Przykładem największych operacji tego typu mogą być operacja Izraela przeciwko syryjskiej obronie powietrznej, wojna rosyjsko - gruzińska i oczywiście rosyjsko-ukraińska, czy też amerykańska kontrofensywa przeciwko ISIS.

Obecnie trudno jest zdefiniować rejestr wirtualnych operacji. Tego typu działania wykroczyły już poza ramy klasycznego szpiegostwa czy działań hakerskich. W przypadku kiedy celem staje się całe państwo, można mówić o proliferacji cyberbroni.

W tej chwili na współczesnym polu walki konieczny staje się kolejny wysoce wyspecjalizowany specjalista – informatyk polowy, na przykład na podobieństwo koordynatora lotnictwa JTAC, sapera, czy chemika.

Wojskowe sieci są dobrze zabezpieczone przed ingerencją z zewnątrz, jednaki i tu możliwe jest przeniknięcie do nich. Na przykład jak do sterylnych komputerów irańskiej elektrowni nuklearnej.

We współczesny świecie, nic nie jest w stanie powstrzymać rozwoju nowych cybertechnologii, przede wszystkim na poziomie infrastruktury krytycznej. Dlatego też tak ważne jest, aby umieć określać potencjalne miejsca ataku, określać jego prawdopodobieństwo i mieć wypracowane procedury minimalizowania szkód. Dobrym przykładem posiadania takich umiejętności jest Ukraina.

Najbardziej rozwinięte państwa świata posiadają w Siłach Zbrojnych odpowiednie struktury, które umożliwiają neutralizację zagrożeń na szczeblu strategicznym i operacyjnym. Działania poszczególnych cyber dowództw są porównywalne z operacjami klasycznych wojsk specjalnych. One również potrzebują doskonale wyszkolonych i wyposażonych specjalistów wykonujących konkretne zadania.

W tym celu wiele państw tworzy nowe struktury dowódcze. Na przykład w Stanach Zjednoczonych poszczególne rodzaje sił zbrojnych mają swoje cyberdowództwa.

Coraz więcej państw powołuje odrębne rodzaje sił zbrojnych i dowództw do przeciwdziałania zagrożeniom w Sieci.

W 2017 roku powstałe w 2009 Dowództwo Cybernetyczne Stanów Zjednoczonych zostało wydzielone i stało się dziesiątym dowództwem wojskowym.

W roku 2017 Niemcy utworzyły Dowództwo Przestrzeni Cybernetycznej i Informacyjnej. W 2016 zwiększyła środki na cyberbezpieczeństwo Wielka Brytania.

Takie działania podejmują także państwa spoza NATO. W 2016 roku w Rosji utworzono wojska informacyjne . Również w 2016 wojska lotnicze Republiki Korei utworzyły nowe centrum cyberbezpieczeństwa.

Również w Polsce od listopada 2018 roku powstaje nowy rodzaj Sił Zbrojnych - Wojska Obrony Cyberprzestrzeni.

Na podstawie ustawy o obronie ojczyzny powstaje Komponent Wojsk Obrony Cyberprzestrzeni, który będzie podlegał Dowódcy Komponentu WOC.

Struktura Wojsk Obrony Cyberprzestrzeni - opiera się na Centrum Operacji Cybernetycznych – istniejącej już w Wojsku Polskim jednostce. Trzykrotnie zwiększy się tam liczba etatów.

Cyberżołnierze to nie jest wojsko przyszłości to są żołnierze operujący już dzisiaj.

Zmiany zachodzą również w Narodowym Centrum Kryptolgii oraz Inspektoracie Informatyki.

Obie instytucje zostały połączone w Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni.

Została również powołana Szkoła Podoficerska Łączności Informatyki w Zegrzu (w miejsce dotychczasowego Centrum Szkolenia Łączności Informatyki) oraz Liceum Informatycznego przy Wojskowej Akademii Technicznej.
Cyber komponent powstaje w WOT – docelowo będzie liczył 100 specjalistów.

Na WAT zostały utworzone studia na kierunku kryptologia, gdzie każdego roku studiuje ponad 100 studentów.
W 2017 roku minister Macierewicz ogłosił zamiar przeszkolenia 1 tys. hakerów (tyle co mają Niemcy, więcej niż Rosja). W Polsce brakuje 50 tys. Informatyków.

Na WAT zostały otwarte studia podyplomowe dotyczące cyberbezpieczeństwa, zwiększone zostały limity na kierunkach kryptologia i cyberbezpieczeństwo, informatyka, elektronika i telekomunikacja oraz systemy informatyczne w bezpieczeństwie. Poświęcone cyberbezpieczeństwu studia wojskowe prowadzi też Akademia Marynarki Wojennej w Gdyni. W 2019 moduł szkoleniowy Legii Akademickiej został rozszerzony o komponent cy-

berbezpieczeństwa.

To tam są szkoleni żołnierze, których głównym zadaniem będzie walka z wirusami komputerowymi, fake newsami, komputerową dezinformacją.

W Polsce pomimo powstania Polskiej Agencji Kosmicznej w dalszym ciągu bardzo poważnym problemem jest rozwój sektora kosmicznego oraz wykorzystanie jego możliwości oraz budowa satelitów. Niestety każdego roku problemy się nawarstwiają i jesteśmy coraz bardziej spóźnieni w stosunku do Europy i świata.

Biorąc pod uwagę podejmowane decyzje i realizowane przedsięwzięcia w zakresie cyberbezpieczeństwa, wydaje się, że powinien powstać jeden silny podmiot który powinien zapewnić spójność polskiej polityki cybernetycznej w kraju i zagranicą realizując strategiczne cele państwa, poprzez reprezentowanie polskiego interesu militarnego, gospodarczego i naukowego na arenie międzynarodowej (UE, NATO, ESA, EUMETSAT, EDA) zapewniając koordynację działań nauki, biznesu i administracji państwowej.

ety, a to często potwierdza sytuacja w Polsce, ale i również na świecie, że inicjatorzy nowych wyzwań bardzo często nie mieli zrozumienia i mieli poważne kłopoty.

Michale Flournoy kandydat prezydenta Joe Bidena na sekretarza obrony w Sta-nach Zjednoczonych podczas przemówienia w Kongresie przedstawiła następujące propozycje modernizacji amerykańskich Sił Zbrojnych: megabity zamiast megaton, cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpraca z pilotowanymi samolotami lub załogowymi okrętami oraz sztuczną inteligencją powinny stanowić podstawę modernizacji Sił Zbrojnych.

Natomiast Premier Wielkiej Brytanii Boris Johnson w marcu 2021 r ocenił, że „siła cybernetyczna rewolucjonizuje sposób, w jaki żyjemy i toczymy wojny, podobnie jak to zrobiły Siły Powietrzne sto lat temu."

W przeszłości bardzo duże kłopoty ze swoimi rewolucyjnymi wizjami mieli gen. Douchet z Włoch czy gen. Mitchell ze Stanów Zjednoczonych. Polski przykład to gen. Zagórski i gen. Rayski, a po wojnie gen. Frey Bielecki, pierwszy polski dowódca WLiOP.

Śmiało można powiedzieć, że niewygodni "prorocy" szybko skończyli nie najlepiej. Często dopiero po śmierci zostali uznani i docenieni.

Czas pokazał i udowodnił, że wszyscy oni, jak i wielu innych, miało dużo racji i mówili prawdę.

Czy również tak będzie obecnie? Czy na pewno obecne nowe wyzwania nie przerosną decydentów? Czy obecnie proces modernizacji Sił Zbrojnych, ale i całego kraju idzie w dobrym kierunku? ◄

Zagrożenia cyberbezpieczeństwa dla infrastruktury lotniczej

Cybersecurity threats to aviation infrastructure

Hanna Dzido

Dr

Katedra Transporty i Logistyki
Wydział Nawigacyjny
Uniwersytet Morski w Gdyni

h.dzido@wn.umg.edu.pl

Streszczenie: Lotnictwo stanowi przykład sektora o rozległych wzajemnych połączeniach i złożoności, wysokim poziomie ekspozycji w mediach oraz kluczowej roli w rozwoju społeczno - gospodarczym państw. Infrastruktura lotnicza (liniowa i punktowa) stanowi elementy infrastruktury krytycznej, przez co podlega szczególnej ochronie. Wobec zachodzących zmian, cyfryzacji wielu procesów w funkcjonowaniu lotnisk, linii lotniczych, obsługi pasażerów, transferu danych bezpośrednio związanych z charakterem lotnictwa, za komponenty infrastruktury lotniczej należy uznać również systemy informatyczne wykorzystywane przez podmioty rynku lotniczego w tym m.in.: lotniska, linie lotnicze, organizacje obsługowe, służby lotniskowe. W artykule przedstawiono zagadnienia cyberbezpieczeństwa w lotnictwie cywilnym oraz główne kierunki działań organów nadzoru nad lotnictwem cywilnym światowego ICAO oraz europejskiego EASA. Autorka przedstawia wiodące dokumenty oraz dotychczasowe działania podjęte w kwestiach zapewnienia cyberbezpieczeństwa w zakresie ochrony danych wszystkich uczestników runku lotniczego opracowane na szczeblu międzynarodowym. Autorka wskazuje inicjatywy ICAO i EASA odnoszące się do cyberprzestrzeni, potrzebę skoordynowania krajowych regulacji z odpowiednimi przepisami dotyczącymi zarządzania bezpieczeństwem i ochroną danych oraz włączenia cyberbezpieczeństwa do państwowych systemów nadzoru nad bezpieczeństwem i ochroną lotnictwa jako części kompleksowych ram zarządzania ryzykiem. W artykule przedstawione zostały również przykłady cyberincydentów w branży lotniczej w kontekście zdarzeń monitorowanych przez Eurocontrol oraz zalecenia dotyczące poprawy zdolności przewidywania, wykrywania, reagowania i łagodzenia cyberzagrożeń w lotnictwie cywilnym.

Słowa kluczowe: *Cyberbezpieczeństwo; Cyberbezpieczeństwo lotnicze; Lotnictwo cywilne; Cyberatak; Infrastruktura cyfrowa; Infrastruktura krytyczna*

Abstract: Aviation is an example of a highly interconnected and complex sector, with a high level of media exposure and a key role in the socio-economic development of countries. Aviation infrastructure (line and point) constitutes elements of critical infrastructure, which is why it is subject to special protection. In view of the ongoing changes, digitization of many processes in the functioning of airports, airlines, passenger service, data transfer directly related to the nature of aviation, IT systems used by aviation market entities, including: airports, airlines , maintenance organizations, airport services. The article presents the issues of cyber security in civil aviation and the main directions of activities of the civil aviation supervision authorities of the global ICAO and the European EASA. The author presents the leading documents and actions taken so far to ensure cyber security in the field of data protection of all participants of the aviation market, developed at the international level. The author points to ICAO and EASA initiatives relating to cyberspace, the need to coordinate national regulations with relevant regulations on data security and protection management, and to include cybersecurity in state aviation safety and security oversight systems as part of a comprehensive risk management framework. The article also presents examples of cyber incidents in the aviation industry in the context of events monitored by Eurocontrol and recommendations for improving the ability to predict, detect, respond and mitigate cyber threats in civil aviation.

Keywords: *Cybersecurity; Aviation cybersecurity; Civil aviation; Cyberattack; Digital infrastructure; Critical infrastructure*

Globalna infrastruktura cyfrowa stanowi obecnie podstawę niemal każdego aspektu życia gospodarczego i społecznego, a tym samym prowadzi do zmiany paradygmatu w wymianie informacji. Unikalność tej zmiany przejawia się nie tylko szybkim rozwojem technologicznym, ale także bezprecedensowym poziomem globalnej wzajemnej łączności systemów i sieci. To wszystko niesie za sobą skutki w postaci stałego wzrostu cyberataków. Lotnictwo stanowi przykład sektora o rozległych wzajemnych połączeniach i złożoności, wysokim poziomie ekspozycji w mediach oraz kluczowej roli w rozwoju społeczno - gospodarczym państw. Infrastruktura lotnicza (liniowa i punktowa) stanowi elementy infrastruktury krytycznej, przez co podlega szczególnej ochronie. Wobec zachodzących zmian, cyfryzacji wielu procesów w funkcjonowaniu lotnisk, linii lotniczych, obsługi pasażerów, transferu danych bezpośrednio związanych z charakterem lotnictwa, za komponenty infrastruktury lotniczej należy

uznać również systemy informatyczne wykorzystywane przez podmioty rynku lotniczego w tym m.in.: lotniska, linie lotnicze, organizacje obsługowe, służby lotniskowe. Ze względu na swój globalny charakter, sektor lotnictwa podobnie jak interakcje systemów i przepływy danych mu towarzyszące, wykraczające poza granice państw i poszczególnych organizacji, podlegają wysokiemu potencjalnemu ryzyku cyberataków. Na przestrzeni lat, zgodnie ze stałym wzrostem zapotrzebowania na efektywną mobilność ludzi i towarów, sektor lotnictwa cywilnego przeszedł kilka transformacji cyfrowych, których celem było wykorzystanie potęgi technologii dla zwiększenia wydajności i efektywności branży. Pozwoliło to na utrzymanie szybkiego tempa wzrostu przy jednoczesnym zachowaniu bezpieczeństwa. Jednocześnie konsekwencją postępu cyfrowego stała się ekspozycja wszystkich interesariuszy sektora na zagrożenie bezpieczeństwa cybernetycznego. Udane cyberataki mogą mieć (mają) negatywny wpływ na ciągłość i bezpieczeństwo świadczenia usług, reputację podmiotów lotniczych, efektywność finansową, bezpieczeństwo ludzi, samolotów, obiektów infrastruktury lotniczej czy sprzętu używanego w obsłudze pasażerów. Dlatego też podejście do zagadnienia cyberbezpieczeństwa oraz zagrożeń dla lotnictwa cywilnego musi przyjąć kompleksowy charakter opierając się na globalnych ramach, implikujących współpracę pomiędzy państwami oraz wszystkimi zainteresowanymi stronami (organami nadzoru lotniczego, służbami, podmiotami rynku lotniczego, podróżnymi).

Forum do rozwijania współpracy międzynarodowej na rzecz cyberbezpieczeństwa lotnictwa cywilnego stwarza zarówno Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) jak i Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA). Prace nad cyberbezpieczeństwem lotniczym, ewoluowały wraz ze wzrostem uzależnienia lotnictwa cywilnego od technologii. Przestrzeń oraz zwierzchnictwo obu instytucji gwarantuje spójność, harmonizację, zgodność z międzynarodowymi priorytetami lotnictwa cywilnego dla międzynarodowej społeczności transportu lotniczego wraz z zapewnieniem objęcia nadzorem wszystkich dziedzin lotnictwa cywilnego.

Działania ICAO w kwestiach cyberbezpieczeństwa

Prace ICAO w zakresie cyberbezpieczeństwa lotnictwa są wszechstronne i złożone. Obejmują one:

- opracowywanie norm i zalecanych metod postępowania (SARP) (Norma 4.9.1 i Zalecana praktyka 4.9.2 w Załączniku 17 – *Ochrona lotnictwa* [8] do Konwencji o międzynarodowym lotnictwie cywilnym (konwencja chicagowska));
- opracowywanie procedur i materiałów pomocniczych;
- zapewnienie, że ramy międzynarodowego prawa lotniczego są odpowiednie do zwalczania cyberataków na lotnictwo cywilne;
- podnoszenie świadomości na temat znaczenia działań z zakresu cyberbezpieczeństwa w lotnictwie cywilnym;
- wspieranie dyskusji na temat cyberbezpieczeństwa lotnictwa na szczeblu krajowym, regionalnym i globalnym;
- rozwijanie inicjatyw wspierających tworzenie i wdrażanie zdolności dotyczących cyberbezpieczeństwa lotnictwa dla państw oraz szerszej społeczności lotniczej.

Znaczenie działań na rzecz cyberbezpieczeństwem w lotnictwie cywilnym zostało dodatkowo podkreślone przez przyjęcie trzech rezolucji zgromadzenia ICAO:

1. Rezolucja A39-19 – *Zajęcie się cyberbezpieczeństwem w lotnictwie cywilnym* z 2016 r., (zastąpiona w 2019 r. rezolucją nr 2)
2. A40-10 – *Zajęcie się bezpieczeństwem cybernetycznym w lotnictwie cywilnym* oraz (zastąpiona w 2022 rezolucją nr 3)
3. A41-19 – *Rozwiązanie problemu cyberbezpieczeństwa w lotnictwie cywilnym*.

Rezolucje zawierają ważne klauzule, które m.in. uznają wzajemne powiązania pomiędzy cyberbezpieczeństwem a bezpieczeństwem, ochroną i wydajnością lotnictwa. Przedmiotem obrad na zgromadzeniach ICAO w zakresie cyberbezpieczeństwa stało się m.in. zapewnienie przekrojowego, holistycznego podejścia do cyberbezpieczeństwa lotnictwa na poziomie krajowym i międzynarodowym. W ramach 41 Zgromadzenia ICAO wezwano państwa do przyjęcia i wdrożenia Konwencji pekińskiej z 2010 r. (Konwencja o zwalczaniu bezprawnych czynów dotyczących międzynarodowego lotnictwa cywilnego [6]) oraz Protokołu pekińskiego z 2010 r. (Protokół uzupełniający do Konwencji o zwalczaniu bezprawnego zajmowania statków powietrznych [7]) jako sposób radzenia sobie z cyberatakami na lotnictwo cywilne.

Działania EASA w kwestiach cyberbezpieczeństwa

EASA opracowała Plan Działania w Zakresie Bezpieczeństwa Cybernetycznego (ang. Strategy for Cybersecurity in Aviation) [2], który został zatwierdzony przez zarząd w listopadzie 2015 r. Od tego czasu EASA pracuje nad jego wdrożeniem. Podjęto szereg inicjatyw mających na celu lepsze przeciwdziałanie zagrożeniom cybernetycznym w lotnictwie, poprawę odporności oraz wspieranie wbudowanych zabezpieczeń. Oprócz swoich instytucjonalnych działań w zakresie stanowienia przepisów, EASA pracuje nad poprawą międzynarodowej współpracy w tej dziedzinie, jak również nad promowaniem wymiany informacji między zainteresowanymi stronami z branży lotniczej. Osiągnięcie cyberodpornego systemu lotniczego i włączenie cyberbezpieczeństwa do obecnego pojęcia bezpieczeństwa wymaga skoordynowanych wysiłków interesariuszy systemu lotniczego. W tym zakresie EASA uczestniczy i przewodniczy Europejskiej Platformie Koordynacji Strategicznej (ang. European Strategic Coordination Platform, ESCP), w skład której

***1**. Komponenty systemu cyberbezpieczeństwa lotniczej infrastruktury krytycznej. Źródło: opracowanie własne*

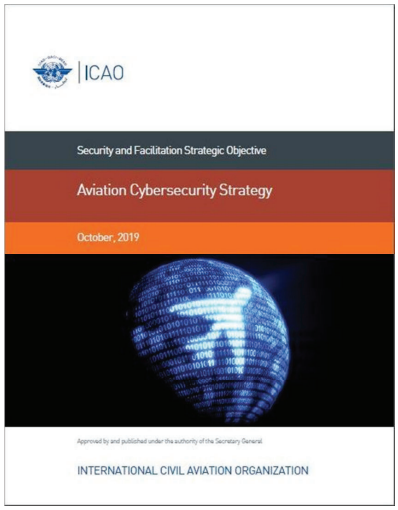
wchodzą przedstawiciele kluczowych zainteresowanych stron z branży, państw członkowskich i instytucji UE. Współpraca przyczynia się do harmonizacji celów interesariuszy lotniczych i umożliwiła opracowanie pierwszej wspólnej strategii cyberbezpieczeństwa w lotnictwie. Zaangażowane zainteresowane strony są również w trakcie określania wspólnego planu działania w celu wdrożenia tej strategii. W celu promocji dobrowolnej wymiany informacji i współpracy ekspertów, EASA wspiera tworzenie Europejskiego Centrum Cyberbezpieczeństwa w Lotnictwie (ECCSA) i zapewnia wstępne zdolności operacyjne we współpracy z CERT-UE.

Strategia Cyberbezpieczeństwa w Lotnictwie Cywilnym według ICAO

Podstawę wizji cyberbezpieczeństwa ICAO stanowi *Strategia bezpieczeństwa cybernetycznego lotnictwa*, zgodnie z którą globalny sektor lotnictwa cywilnego ma być odporny na cyberataki, bezpieczny i chroniony, a jednocześnie nadal zachować możliwości wprowadzania innowacji i rozwoju. Uznając wieloaspektowy i multidyscyplinarny charakter cyberbezpieczeństwa oraz zauważając, że ataki cybernetyczne mogą jednocześnie wpływać na wiele obszarów i szybko się rozprzestrzeniać, konieczna jest wspólna wizja i zdefiniowanie globalnej strategii bezpieczeństwa cybernetycznego. Strategia dostosowana została do innych inicjatyw ICAO związanych z cyberprzestrzenią i skoordynowana z odpowiednimi przepisami dotyczącymi zarządzania bezpieczeństwem i ochroną.

Strategia wyznacza ramy oparte na siedmiu filarach:

1. Współpracy międzynarodowej.
2. Zarządzaniu.
3. Skuteczności ustawodawstwa i przepisów.



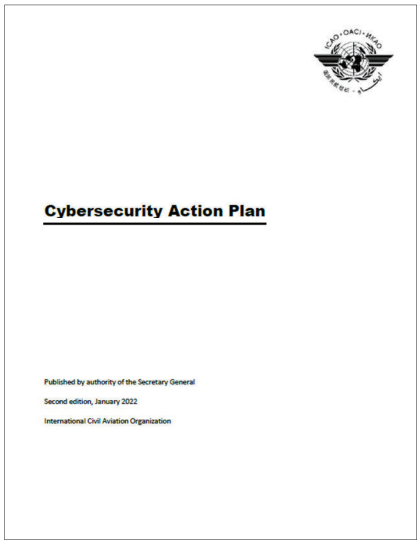
***2**. Publikacja ICAO pt. Strategia Cyberbezpieczeństwa Lotnictwa. Źródło: https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx*

4. Polityce cyberbezpieczeństwa.
5. Udostępnianiu informacji.
6. Zarządzaniu incydentami i planowaniu awaryjnym.
7. Budowaniu potencjału, szkoleniach i kulturze bezpieczeństwa cybernetycznego.

Aspekt współpracy międzynarodowej wynika z ponadgranicznego charakteru zarówno cyberbezpieczeństwa, jak i lotnictwa. Oba wymagają współpracy na poziomie krajowym i międzynarodowym oraz wzajemnego uznawania wysiłków na rzecz rozwoju, utrzymania i poprawy cyberbezpieczeństwa w celu ochrony sektora lotnictwa cywilnego przed wszelkimi cyberzagrożeniami dla bezpieczeństwa i ochrony. Możliwość promocji globalnej spójności i zapewnienia pełnej interoperacyjności środków

***3**. Komponenty ekosystemu lotniczego. Źródło: opracowanie własne*

***4**. Ekosystem lotniczy - interoperacyjność wymiany informacji między użytkownikami. Źródło: Informal Briefing to the ICAO Council, Update on Cybersecurity The Trust Framework, https://www.icao.int/SAM/Documents/2018-GREPECAS18/GRP18_P03.pdf*



***5**. Publikacja ICAO pt. Plan działania w zakresie cyberbezpieczeństwa. Źródło: https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx*

ochrony i systemów zarządzania ryzykiem, wymusza konieczność zharmonizowanych działań na poziomie światowym, regionalnym i krajowym. Państwa członkowskie ICAO, zgodnie ze Strategią Cyberbezpieczeństwa Lotnictwa, muszą sformułować i stosować odpowiednie przepisy ustawowe i wykonawcze zgodne z przepisami ICAO przed wdrożeniem krajowej polityki bezpieczeństwa cybernetycznego w lotnictwie cywilnym.

Cyberbezpieczeństwo ma zostać włączone do państwowych systemów nadzoru nad bezpieczeństwem i ochroną lotnictwa jako część kompleksowych ram zarządzania ryzykiem. W międzyczasie zachęca się państwa do ratyfikowania instrumentów ICAO, w tym: Konwencji o zwalczaniu bezprawnych czynów dotyczących międzynarodowego lotnictwa cywilnego (konwencja pekińska) oraz Protokołu uzupełniającego do Konwencji o zwalczaniu bezprawnego zajmowania statków powietrznych (protokół pekiński).

Z uwagi na fakt istnienia różnych metodologii oceny ryzyka, priorytet należy nadać zmianie i ewentualnemu opracowaniu nowych wytycznych związanych z ocenami zagrożeń i ryzyka dla cyberbezpieczeństwa, w celu osiągnięcia porównywalności wyników takich ocen.

W całym sektorze lotnictwa cywilnego polityka bezpieczeństwa cybernetycznego może uwzględniać pełny cykl życia systemu lotniczego i obejmować takie elementy, jak:

- kulturę bezpieczeństwa cybernetycznego,
- promowanie bezpieczeństwa już w fazie projektowania,
- bezpieczeństwo łańcucha dostaw oprogramowania i sprzętu,
- integralność danych, odpowiednia kontrola dostępu,
- proaktywne zarządzanie lukami w zabezpieczeniach,
- poprawę sprawności aktualizacji zabezpieczeń bez narażania bezpieczeństwa, a także
- włączenie systemów i procesów do monitorowania danych związanych z cyberbezpieczeństwem.

Cyberataki mogą się łatwo rozprzestrzeniać i mieć globalny wpływ. Celem wymiany informacji jest umożliwienie zapobiegania, wczesnego wykrywania i łagodzenia istotnych zdarzeń związanych z cyberbezpieczeństwem, zanim doprowadzą one do szerszych skutków dla bezpieczeństwa lub ochrony lotnictwa. Odpowiednie mechanizmy wraz z kulturą wymiany informacji znacznie zmniejszą systemowe ryzyko cybernetyczne w całym sektorze lotniczym, którego wartość została już udowodniona w zakresie bezpieczeństwa i ochrony lotnictwa. Dzielenie się informacjami na temat takich aspektów, jak słabe punkty, zagrożenia, zdarzenia i najlepsze praktyki, za pośrednictwem ustalonych i zaufanych relacji, może zmniejszyć wpływ trwających ataków.

W kwestii zarządzania incydentami i planowania awaryjnego zgodnie z podejściem ICAO niezbędne jest posiadanie odpowiednich i skalowalnych planów zapewniających ciągłość transportu lotniczego podczas incydentów cybernetycznych. ICAO zaleca, aby państwa i sektor lotniczy korzystały z istniejących planów awaryjnych, które zostały już opracowane i wprowadzały do nich zmiany w celu uwzględnienia przepisów dotyczących cyberbezpieczeństwa. Wysoce zalecane są ćwiczenia w zakresie bezpieczeństwa cybernetycznego jako użyteczne narzędzie do testowania istniejącej odporności cybernetycznej i określania ulepszeń. Ćwiczenia takie mogą mieć różne formaty, np.: ćwiczenia stacjonarne, symulacje lub ćwiczenia w czasie rzeczywistym oraz różną skalę: międzynarodową, krajową, organizacyjną.

Podstawą cyberbezpieczeństwa pozostaje jednak element ludzki. Sektor lotnictwa cywilnego musi podejmować konkretne i skuteczne kroki w celu zwiększenia liczby wykwalifikowanych pracowników posiadających wiedzę zarówno z obszaru lotnictwa, jak i cyberbezpieczeństwa. Cel ten można osiągnąć poprzez zwiększanie świadomości oraz edukację i szkolenia. Programy nauczania związane z cyberbezpieczeństwem oraz cyberbezpieczeństwem lotnictwa na wszystkich poziomach powinny być włączone do krajowych ram edukacyjnych, jak również do odpowiednich międzynarodowych programów szkoleniowych. W lotnictwie należy dążyć do innowacyjnych sposobów łączenia i krzyżowania tradycyjnych technologii informacyjnych i ścieżek kariery w cyberprzestrzeni. Wspieranie i stymulowanie rozwoju umiejętności obecnej i nowej siły roboczej powinno prowadzić do wspierania innowacji w zakresie cyberbezpieczeństwa oraz odpowiednich badań i projektowania rozwiązań dedykowanych branży lotniczej i branż współpracujących.

Lotnictwo cywilne osiągnęło godne pozazdroszczenia wyniki w zakresie bezpieczeństwa (safety i secyrity), które opierają się na proaktywnej kulturze bezpieczeństwa (just culture), którą tworzą i za którą odpowiadają wszyscy. Zasady tej kultury bezpieczeństwa mają być stosowane w celu rozwijania i utrzymywania kultury cyberbezpieczeństwa w całym sektorze lotniczym.

Rezolucja zgromadzenia ICAO A40-10 zwróciła się do ICAO o opracowanie Planu działania w zakresie cyberbezpieczeństwa (ang. Cybersecurity Action Plan CyAP) w celu wsparcia państw i przemysłu w przyjęciu strategii cyberbezpieczeństwa lotnictwa. Pierwsza edycja CyAP została opublikowana w listopadzie 2020 r., a druga w styczniu 2022 r.

CyAP zapewnia podstawę do współ-

pracy ICAO, państw i interesariuszy oraz proponuje szereg zasad, środków i działań, aby osiągnąć cele siedmiu filarów strategii bezpieczeństwa lotniczego. W tym celu CyAP rozwija filary strategii w 32 działaniach priorytetowych, które są następnie podzielone na 51 zadań do wdrożenia przez ICAO, państwa oraz zainteresowane strony.

ICAO kontynuuje opracowywanie materiałów zawierających wytyczne celem dalszego wspierania państw i zainteresowanych stron w zakresie cyberbezpieczeństwa w lotnictwie cywilnym i wdrażania ich obowiązków określonych w normach i zalecanych praktykach ICAO związanych z cyberbezpieczeństwem lotnictwa.

Dotychczas ICAO opublikowało następujące wytyczne:

1. *Rozdział 18 w Podręczniku ochrony lotnictwa ICAO (Doc 8973 – Restricted)*

Rozdział zawiera wytyczne dla państw w zakresie wdrażania ich zobowiązań związanych z normą 4.9.1 w Załączniku 17 – *Ochrona lotnictwa*.

2. Materiał w P*odręczniku ochrony zarządzania ruchem lotniczym* (Doc 9985 – Ograniczony).
   Podręcznik bezpieczeństwa ATM zapewnia całościowe podejście do bezpieczeństwa w środowisku ATM, łącząc wytyczne dotyczące elementów bezpieczeństwa fizycznego i cyberbezpieczeństwa.
3. *Wytyczne dotyczące protokołu sygnalizacji świetlnej.*
   Dokument zawiera wytyczne dotyczące korzystania z protokołu sygnalizacji świetlnej (TLP) w celu ułatwienia wymiany informacji dotyczących cyberbezpieczeństwa. TLP zapewnia prosty i intuicyjny sposób określania przez źródło informacji ograniczeń dotyczących możliwości dalszego udostępniania tych informacji przez odbiorców, minimalizując w ten sposób błąd ludzki polegający na omyłkowym udostępnianiu poufnych informacji poza zamierzonymi odbiorcami.
4. *Wytyczne dotyczące polityki bezpieczeństwa cybernetycznego*
   Dotyczą one ochrony i odporności infrastruktury krytycznej międzynarodowego lotnictwa cywilnego przed zagrożeniami cybernetycznymi oraz wymogu wielostronnej współpracy w lotnictwie cywilnym, a także z organami zewnętrznymi, takimi jak wojsko, organy bezpieczeństwa cybernetycznego i organy bezpieczeństwa narodowego. Materiał zawiera ponadto szablon wspierający opracowanie polityki cyberbezpieczeństwa lotnictwa na poziomie krajowym.
5. *Kultura cyberbezpieczeństwa w lotnictwie cywilnym.*
   Wytyczne opierają się na doświadczeniach lotnictwa cywilnego we wdrażaniu udanych i skutecznych kultur bezpieczeństwa lotniczego i ochrony lotnictwa, łączą odpowiednie elementy z obu kultur i uzupełniają je elementami specyficznymi dla cyberbezpieczeństwa lotnictwa, aby wesprzeć projekt oraz wdrożenie solidnej organizacyjnej kultury cyberbezpieczeństwa w lotnictwie cywilnym.

W ramach działań na rzecz ustalania międzynarodowych ram zaufania lotniczego w 2019 r., kierując się rekomendacją 13 Konferencji Żeglugi Powietrznej, ICAO rozpoczęło prace nad zapewnieniem bezpieczeństwa i odporności systemu żeglugi powietrznej na cyberataki. Działalność ta obejmowała również przechowywanie, przetwarzanie i wymianę danych i informacji spełniającą wymogi poufności, integralności oraz dyspozycyjności. Bieżące prace obejmują opracowanie zasad, polityk i wytycznych dotyczących ram zaufania międzynarodowego lotnictwa (ang. International Aviation Trust Framework IATF). Prace obejmują również zdefiniowanie wymagań wydajnościowych dotyczących przetwarzania, wymiany i przechowywania informacji w aplikacjach sieciowych, w tym opracowanie wymagań technicznych potrzebnych do zaspokojenia obecnych i przyszłych potrzeb lotnictwa.

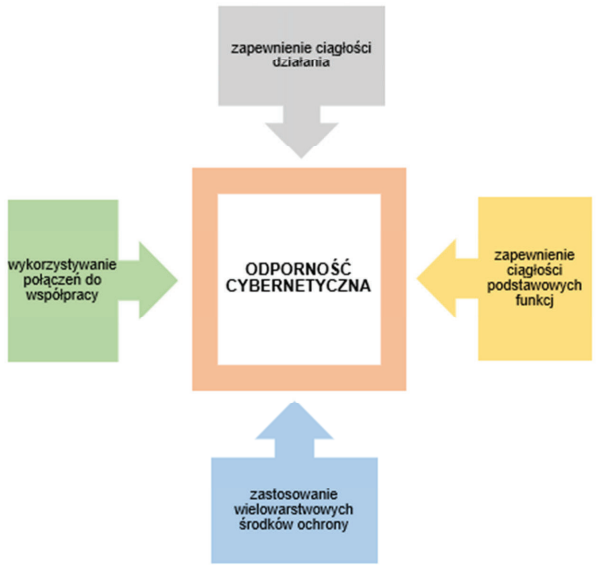
Strategia Cyberbezpieczeństwa w Lotnictwie Cywilnym według EASA

Dokument Strategii Cyberbezpieczeństwa w Lotnictwie (ang. Strategy for Cybersecurity in Aviation) został przyjęty przez Europejską Platformę Koordynacji Strategicznej (ESCP) na krótko przed 40. Sesją Zgromadzenia Ogólnego ICAO. ESCP uznaje znaczenie przeglądu dokumentu strategicznego ESCP z wynikami zgromadzenia oraz zapewnienia spójności i aktualizacji języka odnoszącego się do rezolucji zgromadzenia ICAO w sprawie cyberbezpieczeństwa. Strategia EASA przewiduje przyszły system lotnictwa charakteryzujący się dwoma głównymi udoskonaleniami. Przyszły system lotniczy to:

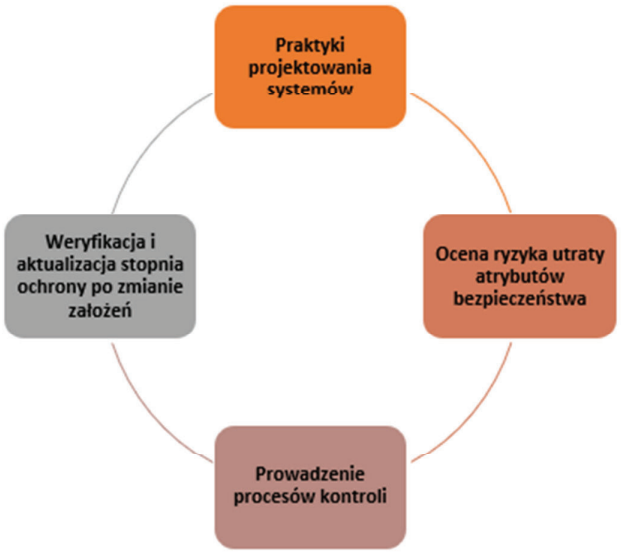
- godnego zaufania i niezawodnego środowiska, aby interesariusze lotnictwa mogli polegać na usługach i informacjach dostarczanych przez innych w celu realizacji swoich celów operacyjnych;
- stworzenie systemu systemów zdolnych do przystosowania się, a tym samym przeciwstawienia się nowym zagrożeniom bez znaczących zakłóceń. System ten ma zostać opracowany poprzez systemowe podejście do cyberbezpieczeństwa w lotnictwie z wykorzystaniem obecnych i starszych systemów.

Osiągnięcie pożądanego ulepszenia, wymaga od zainteresowanych stron z sektora lotnictwa podjęcia wspólnego wysiłku skoncentrowanego na dwóch kierunkach:

1. Uczynienie z lotnictwa ewolucyjnego systemu odpornego na cyberataki, który w przypadku ataku może zachować swoje podstawowe funkcje.
2. Samowzmocnienie lotnictwa poprzez przyjęcie podejścia „wbudowanego bezpieczeństwa", które uwzględnia cele bezpieczeństwa jakie należy osiągnąć od momentu powstania systemów, wraz z tradycyjnymi celami operacyjnymi i bezpieczeństwem.



6. Cele poprawy odporności cybernetycznej wg EASA. Źródło: opracowanie własne



7. Cele samowzmacniającego się systemu lotnictwa wdrażającego wbudowane podejście do bezpieczeństwa. Źródło: opracowanie własne

EASA ustaliła cztery wymierne cele poprawy odporności cybernetycznej:

1. Zapewnienie ciągłości działania dzięki środkom ochronnym rozmieszczonym wzdłuż łańcuchów funkcjonalnych (adekwatnym do poziomu ryzyka),
2. Zapewnienie ciągłości podstawowych funkcji systemów operacyjnych,
3. Stosowanie wielowarstwowych środków ochrony w ramach systemów operacyjnych, które utrudniają postęp ataku,
4. Wykorzystywanie do współpracy istniejących relacji i połączeń w ramach transorganizacyjnego charakteru systemu

oraz cztery wymierne cele dla samowzmacniającego się systemu lotnictwa, wdrażającego wbudowane podejście do bezpieczeństwa:

1. Praktyki projektowania systemów (mają na celu uniknięcie niezamierzonego użycia funkcji dostępnych dla użytkowników),
2. Ocena ryzyka utraty atrybutów bezpieczeństwa oraz wdrożenia środków ochrony, w tym rozwiązań adaptacyjnych,
3. Prowadzenie procesów kontroli (pozwalają na skuteczność bezpieczeństwa systemów w całym cyklu życia),
4. Weryfikacja i aktualizacja stopnia ochrony po zmianie pierwotnych założeń.

Najważniejsze cyberzagrożenia dla branży lotniczej

Branża lotnicza obejmując szerokie spektrum interesariuszy, m.in.: lotnicze, porty lotnicze, służby zarządzania przestrzenia powietrzną, dostawców technologii itp., stanowią jedna z najważniejszych infrastruktur krytycznych wraz z całą jej siecią, zasobami i systemami. Dodatkowo współpracuje również z różnymi branżami podstawowej infrastruktury, w tym z obronnością i bezpieczeństwem narodowym, transportem, komunikacją, bankowością i energią. W rezultacie zakłócenie funkcjonowania branży lotniczej pociąga za sobą negatywne konsekwencje w zakresie zaprowadzenia ładu społecznego i świadczenia usług publicznych.

Przemysł lotniczy, którego działania obejmują skalę międzynarodową obejmując wiele podsektorów, takich jak turystyka i handel zagraniczny, aby sprostać potrzebom tej złożonej struktury musi korzystać z rozwiązań technologicznych. W tym kontekście sektor stopniowo przechodził proces cyfryzacji, przy coraz większym wykorzystaniu innowacyjnych technologii. Pandemia COVID- 19, podobnie jak inne sektory gospodarki, zmusiła branżę lotniczą do implementacji dodatkowych rozwiązań oraz dalszego przeniesienia działalności do sieci. Konsekwencją tak daleko zaistniałej cyfryzacji stała się większa (wzmożona) podatność na cyberataki. Ze względu na charakter branży lotniczej cyberprzestępcy są motywowani dostępem do wrażliwych danych, takich jak paszporty i informacje o kartach kredytowych dużej wartości.

Wśród aktorów stanowiących zagrożenia dla cyberbezpieczeństwa lotniczego można wyróżnić:

- organizacje przeprowadzające ataki sponsorowane przez państwo w celu kradzieży własności intelektualnej i informacji wywiadowczych w celu osłabienia zdolności lotniczych innych krajów, poprawy lokalnych zdolności lotniczych i opracowania technologii zapobiegawczych przeciwko zdolnościom innych krajów [3],
- cyberprzestępcy posiadający niezbędną wiedzę i umiejętności, którzy przeprowadzając ataki koncentrują się na spowodowaniu jak największych szkód,
- cyberterroryści, wywoływani przez czynniki polityczne, religijne, ideologiczne i społeczne. Działania ich skupiają się na zagrożeniu bezpieczeństwa narodowego, powodowaniu masowych ofiar, zaszkodzeniu gospodarce atakowanego państwa, zakłócaniu porządku publicznego oraz podważaniu zaufaniu do systemów lotniczych,
- cyberszpiedzy celujący w przemysł lotniczy, stanowiący jedną z najważniejszych infrastruktur krytycznych. Celem ich działań jest szpiegostwo finansowe, przemysłowe,

politycznego i dyplomatyczne,
- znawcy – tym mianem określani są niezadowoleni pracownicy, byli pracownicy lub partnerzy biznesowi. Motywacją cyberataków z ich strony może być zysk pieniężny lub chęć zemsty,
- aktywiści, którzy nie kierują się względami finansowymi ani politycznymi. Atakują, aby zyskać większy wpływ, rozwinąć umiejętności i uznanie w gronie cyberprzestępców,
- bierni obserwatorzy, działający z zamiarem zebrania informacji. Uzyskują w czasie rzeczywistym obraz ruchu lotniczego i komunikacji z publicznych i prywatnych stron internetowych oraz aplikacji mobilnych, które wyświetlają ruch lotniczy, wykorzystując otwarty charakter protokołów ruchu lotniczego.

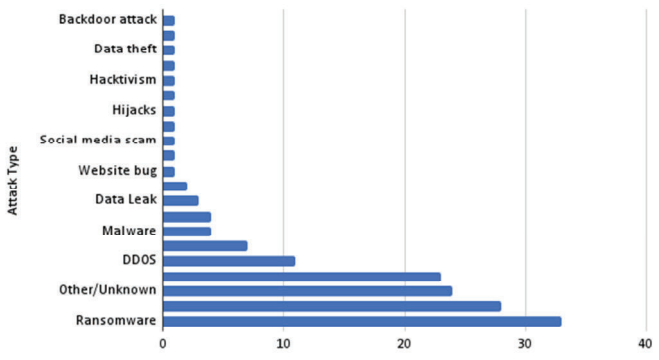
Ataki i luki w zabezpieczeniach

Wykorzystanie złożonych i wzajemnie połączonych systemów informatycznych w przemyśle lotniczym wzrasta z dnia na dzień. Od połączeń Wi-Fi i systemów rozrywki pokładowej dla pasażerów po oprogramowanie używane na lotniskach i liniach lotniczych do zarządzania kontrolą bezpieczeństwa i rezerwacjami - złożone rozwiązania informatyczne są wykorzystywane w całym łańcuchu dostaw przemysłu. Te nowoczesne technologie mają znaczący pozytywny wpływ na systemy sterowania samolotami, poprawiając jakość operacji lotniczych oraz zwiększając bezpieczeństwo i osiągi lotów. Jednak zasila ekosystem, w którym dane przepływają między licznymi interesariuszami a systemami wewnętrznymi/zewnętrznymi. W rezultacie poszerza powierzchnię ataku. Podstawowe technologie stosowane w przemyśle lotniczym można podzielić na kategorie:
- inteligentne systemy,
- urządzenia Internetu rzeczy (ang. Internet of things IoT),
- infrastruktury chmurowe,
- Bigdata,
- Blockchain.

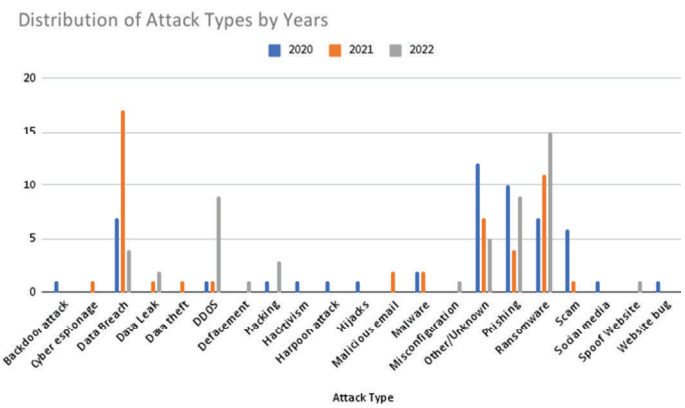
Celem atakujących są zwłaszcza zdalnie atakowane systemy inteligentne (systemy biometryczne, systemy robotyczne itp.), urządzenia IoT (czujniki, siłowniki itp.) oraz systemy chmurowe. Główne systemy często narażone na cyberzagrożenia w branży lotniczej to:
- samolotowe sieci IP lotów,
- cyfrowa kontrola ruchu lotniczego (ATC) i systemy zarządzania ruchem,
- systemy Flight By Wire,
- urządzenia interfejsu podczas lotu,
- serwery historii lotów,
- systemy planowania floty i tras,
- systemy rezerwacji pasażerów oraz programy lojalnościowe lub lojalnościowe,
- portale rezerwacji biletów,
- obsługa i wysyłka ładunków,
- systemy kontroli dostępu, odlotów i paszportów,
- urządzenia personelu pokładowego,
- zagrożenia wewnętrzne.

Cyberataki na przemysł lotniczy w ostatnich latach

W ostatnich latach cyberincydenty w branży lotniczej zostały poddane przeglądowi w kontekście zdarzeń monitorowanych przez Eurocontrol. Eurocontrol (ogólnoeuropejska organizacja cywilno-wojskowa zajmująca się wspieraniem europejskiego lotnictwa) publikuje mapę EATM-CERT (ang. European Air Traffic Management Computer Emergency Response Team) Aviation Cyber Event Map. Dane na tej mapie doprowadziły do następujących ustaleń i wykresów:
- w 2020 r. zgłoszono 52 ataki , w 2021 r. – 48 , a do końca sierpnia 2022 r. – 50 ataków. Tak więc cyberincydenty w 2022 r. osiągnęły średnią z lat 2020 i 2021 zaledwie osiem miesięcy.
- najczęściej obserwowane typy ataków w ciągu ostatnich trzech lat (2020, 2021 i 2022) to ransomware (22 proc.) , naruszenie danych (18,6 proc.) , phishing (15,3 proc.) i DDoS (7,3 proc.). Jako inny/nieznany typ ataku wskazano 16 proc.
- oprócz ataków lotnictwa cywilnego zgłoszono osiem incydentów wojskowych. Niektóre z tych ataków miały na celu cyberszpiegostwo i kradzież danych. Dwa z tych ataków zostały przeprowadzone przy użyciu oprogramowania ransomware , dwa przy użyciu złośliwego oprogramowania, a jeden przy użyciu backdoora. Nie wiadomo, w jaki sposób przeprowadzono trzy z nich.



8. Rodzaje ataków wymierzonych w przemysł lotniczy w latach 2000 - 2022. Źródło: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/



9. Rozkład rodzajów ataków według lat. Źródło: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Tylko w sierpniu 2022 roku miało miejsce siedem ataków. Trzy z nich zostały sklasyfikowane jako wysokie, a cztery jako średnie. Publikowane na ten temat informacje wskazują na naruszenie (zagrożenie) bezpieczeństwa generujące lub mogące wygenerować daleko idące konsekwencje [3]. Wśród przykładowych cyberataków wymienić można:

- cyberatak na portugalską linię lotniczą (TAP Air Portugal), po którym linia lotnicza w wydanym oświadczeniu zapewniła, że jej mechanizmy bezpieczeństwa zostały niezwłocznie aktywowane, a nieautoryzowany dostęp został zablokowany.
- wyciek niektórych baz danych pasażerów linii lotniczych z Malezji i Zjednoczonych Emiratów Arabskich na skutek działań hakerów,
- naruszenie bezpieczeństwa danych osobowych pasażerów Indyjskiej linii lotniczej (Akasa Air), ujawnionych poprzez cyberatak,
- ujawnienie danych osobowych użytkowników aplikacji kanadyjskiej linii lotniczej (WestJet),
- cyberatak, któremu uległa firma American Airlines Group Inc (AAL.O). Zgłosiła ona naruszenie danych na kontach e-mail niewielkiej liczby członków swojego zespołu. Adresy, numery telefonów, numery prawa jazdy, numery paszportów i/lub informacje medyczne mogły uzyskać dostęp do nieautoryzowanych cyberprzestępców.
- cyberatak na linie lotnicze Philippine Airlines. Naruszenie bezpieczeństwa cybernetycznego miało wpływ na zewnętrznego dostawcę IT w ramach programu dla osób często podróżujących. Nazwiska członków, daty urodzenia, narodowość, płeć, data dołączenia, poziom i saldo punktów były wśród naruszonych informacji. Linia lotnicza zaleciła członkom natychmiastową zmianę haseł.
- Ransomware LockBit zaatakował Agencję Bezpieczeństwa Żeglugi Powietrznej w Afryce i na Madagaskarze (ASECNA). Podczas tego bardzo poważnego incydentu dane z 18 krajów członkowskich agencji zostały zaszyfrowane, a agencja zagroziła ujawnieniem naruszonych danych w ciemnej sieci, chyba że zostanie zapłacony okup w wysokości 25 000 USD.

W branży lotniczej, podobnie jak w wielu innych branżach, ewolucja cyfrowa wpływa na wszystkich interesariuszy w ekosystemie lotniczym. Dotyczy zarówno systemów, jak i ludzi, a zmiany w jednym obszarze odczują wszyscy. Cyberprzestępcy kierują się celami finansowymi i politycznymi oraz chęcią zdobycia poufnych informacji. Oprócz ryzyka strat finansowych czy utraty reputacji, udane ataki w sektorze lotniczym mogą spowodować zakłócenia w ruchu lotniczym, wypadki, a nawet utratę życia. Branża lotnicza wykorzystująca liczne rozwiązania technologiczne, celem zapewnienia swoim klientom jak najlepszych doświadczeń użytkowników, musi wykazać się taką samą wrażliwością w wykrywaniu i reagowaniu na cyberzagrożenia.

W tym kontekście dla branży lotniczej można przedstawić zalecenia dotyczące poprawy jej zdolności przewidywania, wykrywania, reagowania i łagodzenia cyberzagrożeń;

- edukacja pracowników w zakresie cyberbezpieczeństwa, a także wyposażenie ich w niezbędne narzędzia o dużej pojemności,
- zidentyfikowanie punktów ryzyka łańcucha dostaw,
- zapewnienie bezpieczeństwa transmisji danych pomiędzy ziemią a samolotem,
- wdrożenie zabezpieczeń dostępu do urządzeń i systemów sieciowych,
- ochrona urządzeń końcowych,
- budowa solidnych systemów zarządzania tożsamością i dostępem z pozycji podmiotu lotniczego oraz z pozycji klienta (podróżnego),
- szyfrowanie wszystkich danych przesyłanych, przechowywanych i przetwarzanych w środowiskach od początku do końca.

Ocena wszystkich systemów lotniczych pod kątem luk w zabezpieczeniach, ustalenie oceny ryzyka i ustalenie priorytetów powinna obejmować kilka elementów. Do niezbędnych zalicza się określenie powierzchni ataku i możliwość ochrony wszystkich zasobów cyfrowych i oszacowanie potencjału wykorzystania informacji pod kątem zagrożenia cybernetycznego oraz do określenia możliwych zagrożeń i proaktywnego reagowania ma kluczowe znaczenie. ◄

Materiały źródłowe

[1] European Strategic Coordination Platform
[2] European Strategic Coordination Platform, Strategy for Cybersecurity in Aviation, First Issue – September 10th, 2019
[3] https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/
[4] https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities#group-easa
[5] https://www.icao.int/aviationcybersecurity/Pages/default.aspx
[6] https://www.icao.int/secretariat/legal/Docs/beijing_convention_multi.pdf
[7] https://www.icao.int/secretariat/legal/Docs/beijing_protocol_multi.pdf
[8] https://www.ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17.pdf
[9] Podręczniku ochrony zarządzania ruchem lotniczym (ICAO Doc 9985)
[10] Rezolucja A39-19 – Zajęcie się cyberbezpieczeństwem w lotnictwie cywilnym z 2016 r.,
[11] Rezolucja A40-10 – Zajęcie się bezpieczeństwem cybernetycznym w lotnictwie cywilnym
[12] Rezolucja A41-19 – Rozwiązanie problemu cyberbezpieczeństwa w lotnictwie cywilnym
[13] Strategy for Cybersecurity in Aviation – Analysis and Objectives

Infrastruktura krytyczna a odporność strategiczna państwa

Critical infrastructure and strategic resilience of the state

Stefan Czmur

Gen. bryg. prof. dr inż.

Streszczenie: W ostatnim okresie pandemia COVID – 19 i wydarzenia związane z agresją Rosji na Ukrainę oraz ogólny wzrost napięcia w stosunkach międzynarodowych poddały surowemu sprawdzianowi systemy bezpieczeństwa globalnego, regionalnego oraz narodowego poszczególnych państw. Doświadczenia z tych wydarzeń dostarczają wielu wniosków, które powinny być wykorzystane w procesie dostosowywania systemów bezpieczeństwa do nowego i wciąż zmieniającego się środowiska polityczno – militarnego, ekonomicznego, społecznego i naturalnego. Doświadczenia te uwypukliły znaczenie odporności strategicznej państwa, a także sojuszy. Znalazło to swoje odbicie w dokumentach normatywnych zarówno narodowych jak i sojuszniczych. W Sojuszu Północnoatlantyckim powołany został Komitet Odporności jako najwyższy organ doradczy ds. odporności strategicznej oraz przygotowania społeczeństwa do funkcjonowania w czasie kryzysu i wojny. W kilku państwach trwają intensywne prace nad stworzeniem strategii odporności państwa powiązanej ze strategią bezpieczeństwa narodowego. W odróżnieniu od tych ostatnich strategie odporności państwa mają za zadania ograniczenie do akceptowalnego poziomu ryzyka zakłócenia najbardziej podstawowych funkcji państwa i społeczeństwa oraz zapewnienie możliwości ich przywrócenia w rozsądnym czasie i za rozsądną cenę

Słowa kluczowe: *Infrastruktura krytyczna; Odporność strategiczna; Bezpieczeństwa narodowe*

Abstract: Recently, the COVID-19 pandemic and the events related to Russia's aggression against Ukraine, as well as the general increase in tension in international relations, have put the global, regional and national security systems of individual countries to a severe test. Experiences from these events provide many conclusions that should be used in the process of adapting security systems to the new and constantly changing political-military, economic, social and natural environment. These experiences have highlighted the importance of the strategic resilience of the state, as well as of alliances. This was reflected in both national and allied normative documents. In the North Atlantic Alliance, the Resilience Committee was established as the highest advisory body for strategic resilience and preparing the society to function in times of crisis and war. In several countries, intensive work is underway to develop a state resilience strategy linked to a national security strategy. Unlike the latter, state resilience strategies are designed to limit the risk of disruption to the most basic functions of the state and society to an acceptable level and ensure that they can be restored in a reasonable time and at a reasonable price.

Keywords: *Critical infrastructure; Strategic Resilience; national security*

Jednym z zasadniczych obszarów, którymi zajmuje się strategia odporności państwa jest budowa odporności strategicznej infrastruktury krytycznej. Wojna w Ukrainie w całej rozciągłości wykazała znaczenie ochrony tej infrastruktury w aspekcie ogólnej odporności państwa i społeczeństwa. Doświadczenia te powinny być starannie przeanalizowane przez odpowiednie organy administracji publicznej i ośrodki naukowe zajmujące się bezpieczeństwem narodowym. Nawet bardzo ogólna analiza stanu i funkcjonowania podstawowych systemów infrastruktury krytycznej w Polsce wskazuje ich niepokojące czułe punkty, które powinny być możliwie szybko wyeliminowane, tak aby poziom ryzyka zakłócenia ich funkcjonowania stał się akceptowalny.

Wśród systemów zaliczanych do infrastruktury krytycznej w Polsce szczególnie wiele słabych punktów wykazuje system zaopatrywania w surowce energetyczne, paliwa i energię elektryczną, a także cieplną. Dobitnym przykładem tej czułości jest fakt, że zniszczenie pięciu największych polskich elektrowni cieplnych pozbawia nasz kraj ¼ mocy systemu energetycznego, a najważniejsze polskie rafinerie oraz nafto - i gazoporty są w promieniu rażenia rosyjskim rakiet krótkiego zasięgu. Wrażliwy jest także polski system transportowy, zwłaszcza na najważniejszej dla Polski osi Zachód – Wschód. W niemal całkowitej zapaści jest system ochrony ludności i obrony cywilnej, który nie jest zgodnie z aktualnym

prawem zaliczany do infrastruktury krytycznej, ale jest systemem bardzo ważnym dla odporności strategicznej państwa, w tym w aspekcie zapobiegania niekontrolowanej masowej migracji ludności. Pozbawiona właściwej ochrony ludność jest bardzo podatna na tego typu zjawisko. Poprawy w dziedzinie odporności wymagają także pozostałe systemy infrastruktury krytycznej, a zwłaszcza ochrony zdrowia, zaopatrywania w wodę i żywność, telekomunikacji i teleinformatyki. Nowego podejścia wymaga też bardzo ważny problem odporności strategicznej sił zbrojnych, a zwłaszcza utrzymywania odpowiedniej armii rezerwowej zdolnej do szybkiego przejęcia funkcji osłabionej pierwszymi uderzeniami armii czynnej. Do właściwego rozwiązana tego strategicznie ważnego problemu jest zbudowanie i odpowiednie zabezpieczenia odpowiedniej infrastruktury sił zbrojnych, zapewniającej m.in. możliwość rozśrodkowania armii czynnej oraz uzbrojenia, sprzętu wojskowego i zasobów materiałowych niezbędnych dla uruchomienia armii rezerwowej. W sumie aby podnieść strategiczną odporność naszego państwa i społeczeństwa konieczne są bardzo pilne działania w wielu dziedzinach.

Dynamiczne zmiany w środowisku bezpieczeństwa, z którymi mamy do czynienia w trzeciej dekadzie XXI wieku poddały weryfikacji systemy bezpieczeństwa państw, a także koalicji, i to zarówno w wymiarze zewnętrznym, jak i wewnętrznym. Praktycznemu egzaminowi poddane zostały w szczególności systemy bezpieczeństwa politycznego, militarnego, ekonomicznego oraz społecznego, w tym zdrowotnego. Pandemia Covid -19 w wymiarze globalnym i epidemie tej choroby w poszczególnych krajach obnażyły słabości zarówno Światowej Organizacji Zdrowia, instrumentu mającego chronić świat przed tego rodzaju zagrożeniem, jak i krajowych systemów ochrony zdrowia. Pandemia ta dotkliwie dotknęła także gospodarkę zarówno światową, jak i poszczególnych krajów, zrywając m.in. ciągi dostaw logistycznych i zakłócając produkcję w wielu branżach, w tym stanowiących lokomotywę gospodarki światowej, jak np. przemysł samochodowy.

Z kolei agresja Rosji na Ukrainę ukazała słabość międzynarodowej architektury bezpieczeństwa zbudowanej kiedyś w innych celach politycznych i niewydolnej w obecnej sytuacji. Okazało się, że mimo ONZ czy też OBWE możliwe jest łamanie umów międzynarodowych i brutalna niesprowokowana agresja na sąsiednie państwo. Agresja totalna wymierzona nie tylko w siły zbrojne napadniętego kraju, ale i w jego naród, gospodarkę, kulturę i oświatę, przy zastosowaniu wszelkich dostępnych instrumentów wojny konwencjonalnej, z groźbą zastosowania broni jądrowej. Siła militarna powróciła na czołowe miejsce listy narzędzi służących osiąganiu celów politycznych. Napięcie w stosunkach międzynarodowych rośnie także w innych częściach świata. Chińskie manewry wojskowe wokół Tajwanu, powrót Al – Kajdy do Afganistanu, nieprzyjazna w stosunku do sąsiadów polityka Iranu, czy też zwiększająca się liczba krajów upadłych lub rządzonych przez dyktatorów. W sumie sytuacja międzynarodowa stała się obecnie najgroźniejsza dla bezpieczeństwa od czasów II wojny światowej.
W takiej sytuacji zasadne jest wyciągnięcie wniosków z wydarzeń z ostatnich kilku lat i wykorzystanie ich do przeglądu systemów bezpieczeństwa. Przeglądu, który powinien być wstępem do przebudowy tych systemów, w niemal we wszystkich znanych obszarach bezpieczeństwa. Dotyczy to także Polski, która stała się państwem przyfrontowym, mocno zaangażowanym w pomoc walczącej Ukrainie, krajem z gospodarką poddaną presji kryzysu wokół surowców energetycznych i sankcji ekonomicznych wymierzonych w Rosję, ale dotykających także naszej gospodarki.

Wśród różnorodnych systemów z obszary bezpieczeństwa do rozważań wybrano infrastrukturę krytyczną, pod kątem jej wpływu na odporność strategiczną państwa. Przy czym ich celem jest ukazanie najważniejszych wniosków dla Polski płynących z doświadczeń z ostatnich lat i naszkicowanie koniecznych działań w obszarze infrastruktury krytycznej, działań wzmacniających odporność strategiczną naszego państwa.

Pojęcie „infrastruktura krytyczna" mocno już zakotwiczyło się w naszym kraju zarówno w naukach o bezpieczeństwie, jak i w praktyce działań administracji publicznej i właścicieli obiektów tę infrastrukturę tworzących. Warto jednak przypomnieć, że jest to pojęcie stosunkowo nowe i pojawiło się w polskim systemie prawnym dopiero po przyjęciu naszego kraju do Unii Europejskiej, kiedy to Polska była zmuszona do transpozycji przepisów prawnych oraz unijnych standardów także w zakresie dotyczącym działalności organów administracji publicznej. W efekcie zorganizowany został system zarządzania kryzysowego, którego zasadnicze ramy zawiera Ustawa z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Przyjęte w tej ustawie rozwiązania mają na celu przeciwdziałanie skutkom zdarzeń kryzysowych o znacznych rozmiarach. Jednocześnie ustawa ta określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zakres działania w tej dziedzinie, jak również zasady finansowania zadań zarządzania kryzysowego [10].

Dla naszych rozważań ważne jest to, że ustawa ta zawiera obowiązującą w polskim prawie definicję terminu „infrastruktura krytyczna". Zgodnie z tą ustawą „infrastruktura krytyczna" to: „{…} systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [9]." W dalszej kolejności ustawa wymienia 11 systemów tworzących infrastrukturę krytyczną [9]. Mimo, wielokrotnych nowelizacji tej

ustawy zarówno definicja jak i lista systemów zaliczanych do infrastruktury krytycznej nie były zmieniane.

Dla dalszych rozważań zasadne jest pytanie, czy przedstawiona w cytowanej ustawie lista obejmuje wszystkie systemy tworzące infrastrukturę krytyczną państwa i czy sama definicja tego terminu jest poprawna. W tym wypadku trzeba zgodzić się ze zdaniem tych, którzy uważają, że nasz system zarządzania kryzysowego, w tym regulacje prawne dotyczą tylko sytuacji kryzysowych związanych z klęskami żywiołowymi oraz zdarzeniami o charakterze terrorystycznym. Inaczej mówiąc system ten jest właściwy tylko dla stanu stałej gotowości obronnej państwa. W przypadku wprowadzenia stanu gotowości obronnej państwa czasu kryzysu (ostatnio z niezrozumiałych powodów oficjalnie zniesionego) lub czasu wojny system ten musiałby zostać zreorganizowany i działać w oparciu o inne regulacje prawne niż te, w których zdefiniowana została infrastruktura krytyczna. Toteż należy także zgodzić się z opinią wyrażoną w Strategii Bezpieczeństwa Narodowego 2020, że jednym z zadań w obszarze bezpieczeństwa państwa i obywateli jest integracja systemu zarządzania bezpieczeństwem narodowym, w tym kierowanie obroną państwa poprzez scalenie dotychczas funkcjonujących systemów, w szczególności kierowania bezpieczeństwem narodowym, zarządzania kryzysowego oraz cyberbezpieczeństwa [8] (s. 13).

W praktyce oznacza to, że lista systemów infrastruktury krytycznej powinna zostać uzupełniona przez systemy, które dotychczasowe prawo zalicza do grupy obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa, których listę zawiera Rozporządzanie Rady Ministrów z dnia 24 czerwca 2003 r., aczkolwiek i ona zawiera tak istotne wykluczenia jak obiekty wytypowane dla organów władzy publicznej na stanowiska kierowania [6]. W tym właśnie kierunku idą zalecenia *Strategii Bezpieczeństwa Narodowego 2020*, które postuluje m.in.: „Dostosować krajowy system zarzadzania kryzysowego do systemu reagowania kryzysu Sojuszu Północnoatlantyckiego tak, aby obejmował również obszar konfliktu polityczno – militarnego i umożliwiał płynne przechodzenie od stanu pokoju do stanu kryzysu i stanu wojny, a także tworzył skuteczne narzędzia do zwalczania i przeciwdziałania zagrożeniom, w tym o charakterze hybrydowym" [8] (s. 13). Uznając te zalecenie za w pełni zasadne w dalszych rozważaniach wzięto pod uwagę poszerzoną listę systemów i obiektów infrastruktury krytycznej obejmującą także te związane z obronnością i bezpieczeństwem wewnętrznym.

W odróżnieniu od „infrastruktury krytycznej państwa" pojęcie „odporność strategiczna państwa" nie ma umocowania w polskim porządku prawnym. Zanim ten termin pojawił się w obiegu naukowym i politycznym naukowcy zajmujący się sprawami bezpieczeństwa używali zbliżonego w znaczeniu pojęcia „siła wewnętrzna państwa". Profesor Ryszard Zięba i doktor habilitowana Justyna Zając w swojej ekspertyzie dotyczącej budowy zintegrowanego systemu bezpieczeństwa narodowego Polski, opublikowanej w 2010 r., posłużyli się właśnie tym terminem podkreślając, iż siła wewnętrzna państwa wyraża się w dwóch cechach, z których pierwszą - stanowi nowoczesna organizacja państwa, sprawność organów administracji publicznej, zdolność mobilizacji do podejmowania nagłych wyzwań i likwidowania zagrożeń, a drugą – jest poziom rozwoju społeczno – gospodarczego warunkujący szybkie i efektywne uruchomienie zasobów i instrumentów polityki bezpieczeństwa [5] (s. 20). Natomiast odpornością strategiczną państwa szerzej na forum publicznym zajął się prof. Stanisław Koziej w połowie drugiej dekady XXI wieku. W 2016 roku w jednej ze swoich publikacji stwierdził, że *Strategia Bezpieczeństwa Narodowego RP* z 2014 r., której profesor był z pewnością głównym twórcą, {…} przywołuje potrzebę budowy strategicznej odporności kraju na wszelkiego rodzaju zagrożenia oraz budowy powszechnego bezpieczeństwa terytorialnego {…}" [7] (s. 84-85). W rzeczywistości we wspomnianej strategii termin ten nie pojawia się, ale faktycznie strategia ta wiele miejsca poświęca budowie odporności Polski na wszelkiego rodzaju zagrożenia. Natomiast w tym samym opracowaniu znajdujemy wyjaśnienie co profesor Koziej rozumie pod pojęciem strategiczna odporność kraju. Jego zdaniem jest to: {…} jego zdolność do oporu i przetrwania agresji" [7] (s. 86). Natomiast wśród sposobów budowy tej odporności profesor wymienia operacyjne przygotowanie terytorium kraju i ochrona obiektów infrastruktury krytycznej [7].

Łatwo zauważyć, iż w rozumienia profesora Kozieja odporność strategiczna państwa (kraju) to sposób na odparcie wszelkiego rodzaju zagrożeń, zagrożeń zdefiniowanych w strategii bezpieczeństwa narodowego. Takie podejście do tego problemu nie jest jednak powszechne. Wśród specjalistów zajmujących się tematem odporności strategicznej państwa zaczyna przeważać zdanie, że budowa tej odporności wymaga oddzielnej strategii, różniącej się w swej istocie od strategii bezpieczeństwa narodowego. Zwolennicy takiego podejścia argumentują, iż we współczesnej erze globalizacji oraz rosnącej nieprzewidywalności środowiska bezpieczeństwa koncepcja bezpieczeństwa narodowego musi ustąpić koncepcji odporności narodowej, a co za tym idzie budowanie bezpiecznego państwa musi być zastąpione budowaniem odpornego państwa. Nie da się bowiem w tych warunkach zapewnić oczekiwanego bezpieczeństwa państwa i społeczeństwa [1] (s. 120-123). W efekcie w kilku krajach, nie rezygnując ze strategii bezpieczeństwa narodowego rozpoczęto prace nad sformułowaniem strategii odporności narodowej. Do tych krajów należą m.in. Kanada, Australia, Niderlandy, Nowa Zelandia, Wielka Brytania oraz USA, spośród

których, trzy pierwsze przyjęły już strategię odporności narodowej powiązaną ze strategią bezpieczeństwa narodowego [1] (s. 114-115).

Autor niniejszego opracowania opowiada się za wyważonym podejściem w tej sprawie. Aby to podejście wyjaśnić autor zacytuje Christiana Fjaedera – uznanego fińskiego eksperta w dziedzinie odporności strategicznej. Jego zdaniem: „Z jednej strony bezpieczeństwo i wytrzymałość to zasadnicze elementy odporności, których szczególnym celem jest zmniejszenie prawdopodobieństwa wystąpienia poważnego zdarzenia i ograniczenia jego skutków, aby uniknąć nieodwracalnych szkód i utraty życia, a także ułatwić skuteczną odbudowę poprzez utrzymywania najbardziej istotnych struktur i zasobów w możliwie nienaruszonym stanie. Z drugiej strony odporność mogłaby być postrzegana jako integralny element bezpieczeństwa narodowego, którego szczególnym celem jest zapewnienie gotowości na nieprzewidziane i nagłe zagrożenia, przeciwko, którym nie jest możliwe lub przynajmniej nieopłacalne wykorzystanie zapobiegawczego podejścia do bezpieczeństwa [1] (s. 123)." Oznacza to, że przy rozważaniach na temat odporności strategicznej celem strategicznym powinno być ograniczenie do akceptowalnego poziomu ryzyka zakłócenia najbardziej podstawowych funkcji przy jednoczesnym zapewnieniu możliwości przywrócenia podstawowych funkcji państwa i społeczeństwa w rozsądnym czasie i za rozsądną cenę.

Jednocześnie autor zgadza się z ogólną definicją pojęcia „odporność infrastruktury krytycznej", wyrażoną w raporcie amerykańskiej the National Infrastructure Advisory Council (NIAC). Definicja ta mówi, że jest to: „Zdolność do zmniejszenia wielkości, wpływu lub czasu trwania zakłóceń funkcjonowania infrastruktury krytycznej [1] (s. 120)." Według tej samej agencji odporność infrastruktury krytycznej ma trzy podstawowe cechy tj. solidność – zdolność do utrzymania funkcji krytycznych i absorpcji skutków w przypadku kryzysu lub zakłóceń; zaradność – zdolność do przygotowania się, reagowania i zarzadzania kryzysem lub zakłóceniami poprzez tworzenie i utrzymania zdolności adaptacyjnych i elastyczności w celu przekierowania zasobów i aktywów, a także szybka odbudowa – zdolność powrotu do normalnego działania (funkcjonowania) tak szybko i tak sprawnie jak to jest możliwe [1]. Tak sformułowane cechy odpornej infrastruktury krytycznej w pełni weźmiemy pod uwagę w toku dalszych rozważań.

Odporność strategiczna państwa stała się w ostatnich kilku latach przedmiotem zainteresowania najważniejszych gremiów odpowiedzialnych za bezpieczeństwo zarówno w wymiarze krajowym jak i międzynarodowym. Wzmiankowana już *Strategia Bezpieczeństwa Narodowego RP – 2020* omawiając jeden z filarów bezpieczeństwa narodowego za jaki uznano zarządzanie bezpieczeństwem narodowym zakłada, że jednym z zadań w tym zakresie jest: {…} podniesienie odporności państwa na zagrożenia, poprzez tworzenie systemu obrony powszechnej, opartego na wysiłku całego narodu oraz budowanie zrozumienia dla rozwoju odporności i zdolności obronnych Rzeczypospolitej Polskiej" [8] (s.15). Wśród postulowanych konkretnych szczegółowych zadań związanych z budową odporności państwa wymienione są także, te związane z infrastrukturą krytyczną. Wzmiankowana strategia postuluje bowiem m.in. zwiększenia odporności na zagrożenia przede wszystkim w zakresie: ciągłości rządzenia i funkcjonowania państwa, skutecznych dostaw energii, niekontrolowanego przepływu osób i relokacji ludności, gromadzenia, ochrony oraz zagospodarowania zasobów żywności i wody, zdolności do postępowania w przypadku wystąpienia zdarzeń o charakterze masowym, odpornych sieci telekomunikacyjnych i systemów teleinformatycznych, systemów informowania i ostrzegania ludności oraz wydolnego systemu transportowego [8] (s. 16). Biorąc pod uwagę doświadczenia wojny w Ukrainie tak sformułowane zadanie należy uznać za trafne. Natomiast w całym zestawie przedsięwzięć, obejmujących 20 postulowanych zadań, brakuje – zdaniem autora – zadań związanych z tak istotnym elementem odporności strategicznej państwa jakim jest zdolność do szybkiej i efektywnej odbudowy sił zbrojnych poprzez stworzenie wszelkich koniecznych warunków do zbudowania odpowiednich rezerw osobowych i materialnych. Nie ulega bowiem wątpliwości, że poważne straty czynnej części sił zbrojnych i możliwie szybka odbudowa ich podstawowych zdolności muszą być brane pod uwagę w rozważaniach nad bezpieczeństwem państwa. W omawianej strategii problemom sił zbrojnych jest poświęcona jej kolejna część, ale dotyczy ona wzmocnienia zdolności operacyjnych Sił Zbrojnych RP do odstraszania i obrony przed zagrożeniami bezpieczeństwa, ze szczególnym uwzględnieniem podniesienia poziomu mobilności i modernizacji technicznej [8] (s.18-19). Tymczasem chodzi o stworzenie armii rezerwowej wykorzystanej w razie potrzeby do efektywnej i szybciej odbudowy czynnych sił zbrojnych.

W środowisku NATO odporność strategiczna ma swoje umocowanie w postaci artykułu 3 Traktatu Północnoatlantyckiego, a ponowne skupienie się na tej odporności zostało zapoczątkowane podczas Szczytu NATO w Warszawie odbytego w dniach 8 .- 9 lipca 2016 r. Jednym z przyjętych wówczas przez głowy państw i rządów dokumentów strategicznych był dokument zatytułowany „Zobowiązanie do zwiększenia odporności" (Commitment to enhance resilience). Zwrócono w nim uwagę na szczególne znaczenie budowy odporności państw sojuszniczych na pełne spektrum zagrożeń zarówno tych o charakterze militarnym jak i niemilitarnych. W punkcie czwartym tego dokumentu odczytać można istotę odporności strategicznej w odniesieniu do NATO. Zapisano w nim

m.in.: „Odnotowując, iż gotowość społeczeństwa jest przede wszystkim obowiązkiem krajów członkowskich, będziemy dążyć do uzgodnionych wymogów dotyczących odporności narodowej. Będziemy chronić naszą ludność i terytorium wzmacniając ciągłość rządzenia, ciągłość podstawowych usług i bezpieczeństwo cywilnej infrastruktury krytycznej; i będziemy pracować nad tym, aby nasze narodowego i sojusznicze siły zbrojne mogły być zawsze odpowiednio wspierane zasobami cywilnymi, w tym energią, transportem i łącznością [3]." Jak łatwo zauważyć infrastruktura krytyczna znalazła się w centrum uwagi najwyższego sojuszniczego gremium ze szczególnym naciskiem na systemy energetyczny, transportowy i łączności.

Jednym z efektów cytowanego dokumentu było powołanie Komitetu Odporności (Resiliance Committee) jako najwyższego organu doradczego NATO ds. odporności i przygotowania społeczeństwa. Dzięki pracom w/w komitetu 14 czerwca 2021 r. na kolejnym szczycie NATO w Brukseli głowy państw i szefowie rządów wydali dokument zatytułowany: „Wzmocnienie zobowiązań dotyczących odporności" (Strengthened Resiliance Commitment). Lektura tego dokumentu jednoznacznie wskazuje, że odporność strategiczna jest łączona z przygotowaniem społeczeństwa i jest podstawowym sposobem na przygotowanie państwa członkowskich NATO i całego sojuszu do skutecznego przeciwstawienia się całemu spektrum zagrożeń i wyzwań zarówno o charakterze militarnym, jak i niemilitarnym, w tym hybrydowych. W punkcie ósmym tego dokumentu podkreślono, iż: „Zwiększymy nasze wysiłki na rzecz zabezpieczenia i dywersyfikacji naszego łańcucha dostaw, a także zapewniania odporności naszej infrastruktury krytycznej (na lądzie, morzu, w kosmosie i cyberprzestrzeni) oraz kluczowych gałęzi przemysłu, w tym poprzez ich ochronę przed szkodliwą działalnością gospodarczą" [4]. Powyższy cytat potwierdza, że w ocenie najwyższego gremium decyzyjnego NATO odporność infrastruktury krytycznej jest jednym z najważniejszych zadań poszczególnych państw członkowskich i całego NATO.

Komitet Odporności NATO jest wspierany przez sześć wyspecjalizowanych grup planowania. Przeznaczenie tych grup jednoznacznie wskazuje obszaru skupienia głównego wysiłku NATO w zakresie odporności strategicznej. Są to kolejno grupy:

1. Grupa Planowania Komunikacji Cywilnej (Civil Communications Planning Group – CCPG) - doradzająca w zakresie budowy odporności sektora komunikacji;
2. Grupa Ochrony Ludności (Civil Protection Group – CPG) - zajmująca się sposobami zapewnieni ciągłości rządzenia oraz zdolnością do skutecznego radzenia sobie z niekontrolowanymi przepływami ludności;
3. Grupa Planowania Energetycznego (Energy Planning Group – EPG) – odpowiadająca za doradztwo w zakresie stabilnych dostaw energii;
4. Grupa Planowania Wyżywienia i Rolnictwa (Food and Agriculture Planning Group) zajmująca się kwestiami odporności w sektorze żywności i wody;
5. Połączona Grupa Zdrowia (Joint Health Group – JHG) zajmująca się zdolnością członków NATO do radzenia sobie z masowymi ofiarami i destrukcyjnymi kryzysami zdrowotnymi;
6. Grupa transportowa (Transport Group – TG) doradzająca w zakresie budowy odporności systemu transportu cywilnego z podziałem na transport, lądowy, morski i powietrzny.

Przegląd zakresu odpowiedzialności grup planowania pracujących na rzecz Komitety Odporności NATO jest jednoznaczną referencją na jakich obszarach powinny skupić się nasze narodowe gremia decyzyjne w zakresie odporności strategicznej państwa. Kompatybilność prac gremiów sojuszniczych i narodowych w tym zakresie przyniosłaby bez wątpienia efekt synergii w końcowych rezultatach prac naszych zespołów krajowych, które pracowałyby na rzecz rozwiązywania problemów w skali całego NATO i jednocześnie wykorzystywałyby wyniki prac grup sojuszniczych do rozwiązywania tych problemów w naszym kraju.

Po ustaleniu istoty pojęcia „odporność strategiczna państwa" oraz jej związków z ochroną infrastruktury krytycznej wynikających z treści krajowych i sojuszniczych dokumentów normatywnych możemy przejść do oceny aktualnej odporności strategicznej Polski. W literaturze przedmiotu trudno jest znaleźć bezpośrednią ocenę poziomu odporności strategicznej Polski bądź tzw. siły wewnętrznej państwa. Na ogół autorzy dokonują cząstkowych ocen, z których nie zawsze można złożyć ogólny obraz. Jeśli jednak taka ocena jest wystawiona przeważa zdanie, że poziom odporność naszego kraju jest średni. Do słabości zalicza się np. niewłaściwą organizację systemu ratownictwa, niewydolny system ostrzegania i alarmowania, upolitycznienie służb specjalnych skutkujące karuzelą kadrową negatywnie wpływającą na efekty ich działania itp. [5] (s. 20-21) Jak łatwo zauważyć są to czynniki trudne do zmierzenia i precyzyjnego oszacowania.

Łatwiej sprawa wygląda w stosunku do większości systemów infrastruktury krytycznej, w przypadku, których możliwe jest wykorzystanie wskaźników ilościowych. Takim przypadkiem jest system zaopatrywania w energię, surowce energetyczne i paliwa. Wystarczy porównać zapotrzebowania np. na surowce energetyczne i paliwa, z produkcją krajową, aby dostrzec jak wrażliwa jest to kwestia dla Polski. W 2020 roku Polska zużyła 52 153 tys. t węgla energetycznego, 25 757 t ropy naftowej oraz 18 366 mln m3 gazu, importując odpowiednio: 11 056 tys. t węgla (21.2%), 24 906 tys. t ropy (96,7%) i 16 510 mln m3 gazu (89,7%). Przy czym mimo wysiłków zmierzających do dywer-

syfikacji źródeł pozyskiwania tych surowców, dominującym krajem ich pochodzenia była Rosja, która sprzedała Polsce 9 448 tys. t węgla energetycznego, 16 396 mln t ropy naftowej oraz 9 049 mln m3 gazu ziemnego (łącznie z gazem z Azerbejdżanu) co stanowiło odpowiednio 18,1% zapotrzebowania Polski ma węgiel energetyczny, 63,7% zapotrzebowania na ropę i 49,3% zapotrzebowania na gaz ziemny (Obliczenia własne na podstawie danych z Rocznika „Gospodarki Surowcami mineralnymi w Polsce w 2020" IGSMiE PAN). Agresja Rosji na Ukrainę spowodowała, iż Rosja przestaje być dostawcą surowców energetycznych do Polski, ale nasz kraj – mimo trudności - jak dotąd znalazł alternatywne źródła tego rodzaju surowców. Jednak towarzysząca temu gwałtowna podwyżka cen spowodowana głównie światowym kryzysem energetycznym wywołanym wojną w Ukrainie stawia pytanie czy koszt tej zmiany będzie akceptowalny dla gospodarki polskiej i polskiego społeczeństwa. Dopiero wtedy uzyskamy odpowiedź na pytania czy nasz system zaopatrywania w surowce energetyczne jest odporny strategicznie.

Rosnące koszty surowców energetycznych to nie jest jednak w szerszej perspektywie najważniejszy problem odporności naszego systemu zaopatrywania w energię, surowce energetyczne i paliwa. System ten ma bowiem kilka bardzo czułych punktów związanych z transportem surowców energetycznych, produkcją paliw i energii elektrycznej. Są to punkty, które czynią Polskę bardzo wrażliwą w przypadku kryzysu polityczno – militarnego i wojny. Dwie czołowe inwestycje związane z dywersyfikacją dostaw gazu ziemnego, czyli gazociąg bałtycki i gazoport w Świnoujściu są związane z morzem. Gazociąg biegnący po dnie Morza Bałtyckiego może być łatwo zniszczony (co potwierdza przypadek uszkodzenie gazociągów Nordstream 1 i 2) przez siły morskie i specjalne Rosji. Transport LNG drogą morską i jego rozładunek w Świnoujściu także może zostać zablokowany od strony morza, a instalacje służące rozładunkowi i dalszemu transportowi gazu lądem zniszczone w wyniku uderzenia rakietowego lub przy użyciu lotnictwa. Polska samodzielnie nie jest obecnie w stanie zapewnić tym instalacjom odpowiedniego bezpieczeństwa. Konieczne jest wsparcie sojuszników z NATO.

Z kolei paliwa płynne produkowane w Polsce pochodzą w zdecydowanej większości z rafinerii w Płocku i Gdańsku, przy czym ta ostatnia rafineria jest uzależniona od dostaw ropy naftowej drogą morską przez naftoport w Gdańsku. Wszystkie te trzy instalacje są położone od rosyjskiego Obwodu Kalingradzkiego w odległości umożliwiającej użycie do ich zniszczenia rakiet małego zasięgu lub dronów. Jest to więc swoista pięta Achillesa polskiego systemu zaopatrywania w paliwa. To wszystko musi być uwzględnione przy rozpatrywaniu odporności strategicznej Polski. Polska musi założyć wariant niszczącego uderzenia na zasadnicze obiekty związane z transportem gazu ziemnego droga morską i produkcji paliw płynnych i poszukać rozwiązania umożlwiającego przetrwania naszego kraju w tych niekorzystnych warunkach. Wydaje się, że najlepszym rozwiązaniem byłoby zwiększanie podłączeń polskich rurociągów i gazociągów do europejskiej sieci gazowej i paliwowej.

Nie mniej wrażliwy jest także polski system energoelektryczny. W 2020 roku cała produkcja tego systemu wyniosła 157,7 TWh, z czego 125,9 TWh, czyli 80% wyprodukowały elektrownie cieplne, z tego 46% pracujące na węgiel kamienny i 24% - na węgiel brunatny. Tylko 18% energii pochodziło z elektrowni wytwarzających prąd z odnawialnych źródeł energii [11]. Zasadniczym problemem jest koncentracja zainstalowanych mocy w elektrowniach cieplnych. W 2022 r. moc wszystkich elektrowni Polsce wynosiła prawie 60 000 MW (59 578 MW), z tego blisko 27 000 MW mocy (45%) pochodziło z 20 największych elektrowni cieplnych na węgiel kamienny i brunatny. Pięć polskich największych elektrowni cieplnych (Bełchatów, Kozienice, Opole, Połaniec i Rybnik) ma moc 16 142 MW [2]. Ich zniszczenie to eliminacja 26,9% mocy polskich elektrowni. Przy obecnych precyzyjnych środkach rażenia rakietowych i lotniczych zniszczenie tych kliku elektrowni może nie być zbyt trudne jeśli nie zostaną one odpowiednio zabezpieczone środkami obrony powietrznej i przeciwrakietowej. Perspektywa budowy elektrowni jądrowych w Polsce prawdopodobnie zwiększy wrażliwość naszego systemu elektroenergetycznego. Będę to bowiem instalacje energetyczne o dużej mocy, których eliminacja spowoduje gwałtowne spadek produkcji energii elektrycznej. Z drugiej strony doświadczenia z wojny w Ukrainie wskazują, że potencjalny agresor musi brać pod uwagę negatywne skutki zniszczenia elektrowni jądrowych, w postaci promieniotwórczego skażenia także własnego terytorium. Nie mniej generalnie najlepszym sposobem zwiększenia odporności systemu energoelektrycznego jest zwiększenie udziału odnawialnych źródeł energii produkowanych w dużej sieci stosunkowo małych elektrowni. Drugim sposobem jest odpowiednie podłączenia do europejskiego systemu energetycznego umożlwiającego w razie potrzeby import znacznych ilości energii elektrycznej.

Systemy transportu w Polsce, także wymagają przedsięwzięć podnoszących ich odporność. Bardzo wrażliwy pod tym względem jest transport morski, którego dwa spośród trzech zasadniczych portów są w zasięgu rosyjskich rakiet krótkiego zasięgu. Bez pomocy sojuszniczych sił morskich Polska nie jest w stanie także zapobiec ich blokadzie ze strony marynarki wojennej Federacji Rosyjskiej. Z kolei w systemie transportu lądowego, najbardziej istotne jest utrzymanie sprawności i przepustowości artylerii Zachód – Wschód, niezbędnych do sprawnego przerzutu zgrupowań wojsk sojuszniczych i własnych oraz zapewnienia łańcucha

dostaw logistycznych dla zgrupowań rozmieszczonych w północno – wschodnie części naszego kraju. W przypadku konfliktu zbrojnego system ten nabierze szczególnego strategicznego znaczenia, na co zwrócił już kiedyś uwagę, aczkolwiek w innych realiach politycznowojskowych, pułkownik Ryszard Kukliński. Tymczasem system transportu kolejowego ma dwie systemowe słabości. Pierwsza jest związana z innych rozstawem szyn na naszej wschodniej granicy, w tym z Litwą i Ukrainą, tak ważnych dla nas partnerów strategicznych. Natomiast na granicy z RFN barierą jest odmienność systemu zasilania lokomotyw elektrycznych, wymuszająca stosowanie lokomotyw z dwoma rodzajami silników elektrycznych. Ponieważ przebudowa naszego systemu wymagałaby dużych nakładów finansowych, należałoby zastanowić się nad rozwiązaniami niezbędnymi do zwiększenia przepustowości linii kolejowych przechodzących przez naszą granicę zachodnią. W przyszłości natomiast należałoby stopniowo dostosowywać nasze linie kolejowe do systemu obowiązującego Europie Zachodniej.

W transporcie drogowym, ale także kolejowym problemem jest jego kanalizacja na linii trzech rzek tj. Wisły, Warty i Odry. Z powodu tych rzek stworzone zostały odpowiednie przeprawy drogowe i zazwyczaj im towarzyszące przeprawy kolejowe. Doprowadziło to do stworzenia kilku dużych węzłów drogowo – kolejowych obejmujących przeprawy przez szerokie przeszkody wodne, i zazwyczaj posiadających także duże lotnisko komunikacyjne. Największe tego typu węzły to węzły: aglomeracji warszawskiej z sześcioma lotniskami komunikacyjnymi, wojskowymi i sportowymi, aglomeracji poznańskiej, aglomeracji wrocławskiej oraz bydgosko – toruńskiej i szczecińskiej. Wielkie znaczenia ma także kilka przepraw drogowo – kolejowych przez Wisłę (Tczew, Grudziądz, Włocławek, Płock, Dęblin) oraz Odrę (Kostrzyn, Rzepin – Świecko, Cigacice, Brzeg). Podstawowym sposobem podniesienia odporności tych węzłów powinna być ich obrona przeciwrakietowa oraz przedsięwzięci ukierunkowane na szybką odbudowę przepraw i przygotowanie przepraw tymczasowych.

Wojna w Ukrainie po raz kolejny pokazała wagę systemu ratownictwa oraz ściśle z nim powiązanego systemu ochrony ludności i obrony cywilnej. Jak już wcześniej wspomniano ze względu na „pokojowy" charakter systemu zarządzania kryzysowego ochrona ludności w przypadku wojny i obrona cywilna są w naszym kraju poważnie zaniedbane. Nie ma nawet odpowiednich regulacji prawnych. W Ustawie o powszechnym obowiązku obrony RP z 1967 roku był cały dział poświęcany obronie cywilnej. Wprowadzone w jej miejsce Ustawa o obronie Ojczyzny z 11 marca 2022 roku nie zawiera regulacji dotyczących obrony cywilnej. W obliczu doświadczeń z wojny w Ukrainie dalsze zwlekania z prawnym uregulowaniem tego problemu jest całkowicie niezrozumiałe. Tym bardziej, że wzmiankowana już *Strategia Bezpieczeństwa Narodowego 2020* zawiera bardzo istotny postulat zredefiniowania i przebudowy systemu obrony cywilnej i ochrony ludności [8] (s. 16). Znaczenie tych dwóch elementów odporności państwa i społeczeństwa podkreślają też wspomniane już dokumenty normatywne NATO. Wiele miejsca tym problemom poświęca również Unia Europejska.

W tym miejscu trzeba wyraźnie podkreślić, że zaniedbania w zakresie ochrony ludności i obrony cywilnej w prostej linii prowadzą do niekontrolowanej masowej migracji przemieszczeń ludności w przypadku kryzysu i wojny. Obrona przed tego typu masowym zdarzeniem jest jednym z podstawowych zadań budowy odporności państwa i społeczeństwa. W tym kontekście należy także zauważyć, że dwa podstawowe w Polsce systemy ratownicze, tj. Krajowy System Ratowniczo – Gaśniczy oraz Państwowe Ratownictwo Medyczne mają organizację oraz możliwości działania obliczone na okres pokoju i bez większych katastrof naturalnych. Epidemia COVID -19 obnażyła słabości zwłaszcza ratownictwa medycznego. W sumie istnieje pilna potrzeba stworzenia systemu ratownictwa, ochrony ludności i obrony cywilnej zapewniającego odpowiednią odporność strategiczną naszego państwa i społeczeństwa.

Brak ustalonych wskaźników ilościowych uniemożliwia precyzyjne odniesienie się do pozostałych systemów infrastruktury krytycznej. Nie mniej nawet ogólne spojrzenie na te systemy prowadzi do wniosku, że należy starannie ocenić ich odporność strategiczną. Dotyczy to zwłaszcza systemu finansowego, łączności i sieci teleinformatycznych, zaopatrzenia w żywność i wodę oraz zapewniającego ciągłość funkcjonowania administracji publicznej.

W końcowej części rozważań autor chciałby powrócić do bardzo ważnego elementu odporności strategicznej państwa jakim jest odporność jego sił zbrojnych. Wojna w Ukrainie po raz kolejny udowodniła jak ważnym problemem jest rozśrodkowania armii czynnej chroniące ją przed nadmiernymi stratami w wyniku pierwszego uderzenia oraz istnienie armii rezerwowej służącej do szybkiej odbudowy i rozbudowy armii czynnej. Przy czym przez armię rezerwową należy rozumieć rezerwy osobowe, zapasy sprzętu i uzbrojenia wojskowego oraz całej gamy materiałów logistycznych, w tym zwłaszcza amunicji i paliwa. Nie jest tajemnicą, że Ukraina bez wsparcia ze strony państwa NATO i UE oraz krajów partnerskich obu organizacji nie byłaby już w stania prowadzić działań obronnych z powodu wyczerpania zapasów amunicji i różnego rodzaju materiałów wojskowego przeznaczenia. W sumie odpowiedni poziom odporności strategicznej sił zbrojnych wymaga m.in. odpowiednio rozbudowanej infrastruktury o przeznaczeniu obronnym. Tymczasem w Polsce po wstąpieniu do NATO w wyniku transformacji naszych sił zbrojnych, w trosce o zmniejszanie kosztów utrzymania jednostek woj-

skowych, w pierwszej dekadzie XXI wieku, zamknięto wiele garnizonów, w tym lotnisk, zwłaszcza w zachodniej i środkowej części kraju. W tej chwili nasze państwo stoi w obliczu odbudowy zasobów infrastruktury obronnej, tak aby było możliwe rozśrodkowanie – w razie konieczności – sil zbrojnych, zwłaszcza lotnictwa, sprawne przyjęcia sojuszniczych jednostek wzmocnienia, przerzucanych do naszego kraju, w tym także drogą powietrzną, a także szybkie uruchomienie produkcji specjalnej, zwłaszcza amunicji. Na uwadze trzeba mieć także konieczność stworzenia odpowiednio rozbudowanej bazy szkoleniowej rezerw i formowania jednostek. W tym zakresie należałoby wziąć pod uwagę także możliwość współpracy z krajami sojuszniczymi dysponującymi odpowiednimi zasobami w tym zakresie.

W podsumowaniu autor chciałby przedstawić najważniejsze, jego zdaniem, konkluzje. Po pierwsze - globalizacja współczesnego świata i postępująca nieprzewidywalność współczesnego środowiska bezpieczeństwa wskazują, że Polska powinna oprócz strategii bezpieczeństwa narodowego posiadać odrębną, ale z nią powiązaną, strategię odporności strategicznej, w której jednym z najważniejszych zagadnień powinna być odporność infrastruktury krytycznej. Po drugie – przy rozważaniach dotyczących infrastruktury krytycznej, pod uwagę należy wziąć nie tylko systemy ujęte w aktualnym porządku prawnym, ale także te, które dotyczą obszarów obrony i bezpieczeństwa publicznego. Po trzecie – przy rozpatrywaniu odporności infrastruktury krytycznej należy zdefiniować najważniejsze zmienne dotyczące jej stanu oraz wskaźniki służące pomiarowi tych zmiennych. Po czwarte – biorąc pod uwagę doświadczenia z ostatnich lat, a w szczególności z agresji Rosji na Ukrainę oraz epidemii Covid – 19, zmian klimatu, a także wcześniejszych kryzysów ekonomicznych największą uwagę należy poświęcić takim systemom infrastruktury krytycznej jak: zaopatrywania w energię, surowce energetyczne i paliwa, transportowy, ochrony zdrowia, ratownictwa i ochrony ludności oraz zaopatrywania w wodę i systemów teleinformatycznych i łączności. Po piąte – w systemie zaopatrywania w energię, surowce energetyczne i paliwa, trzeba zadbać przede wszystkim o pewność źródeł zaopatrywania w surowce energetyczne, bezpieczeństwo transportu tych surowców oraz usunięcie wąskich gardeł w ich transporcie, a także zbudowanie wielokierunkowych międzynarodowych powiązań polskiej sieci energetycznej oraz gazociągów i rurociągów z odpowiednimi systemami najważniejszych i pewnych sojuszników. Konieczne jest także znaczące powiększanie zdolności magazynowania gazu i paliw płynnych, w oparciu o właściwie zabezpieczone przed atakami z powietrza magazyny. Po szóste – koniecznym jest opracowanie planu odbudowy i wzmocnienia Sił Zbrojnych RP, w oparciu o odpowiednio rozproszoną i zabezpieczoną infrastrukturę wojskową, w tym także położoną w krajach sojuszniczych. Istotne jest również powiększenia zasobów infrastruktury służącej celom wojskowym, tak aby w krótkim czasie możliwe było rozśrodkowanie czynnych sił zbrojnych, a także materiałów i zasobów mobilizacyjnych oraz przyjęcie znaczących sił wzmocnienia z innych państw NATO. Po siódme – konieczne jest przeprowadzenie przeglądu procedur ochrony (a także obrony) infrastruktury krytycznej, zwłaszcza pod kątem realnych potrzeb w zakresie sił ochrony oraz zdolności odbudowy poszczególnych systemów, a także usunięcia wszelkich biurokratycznych przeszkód blokujących inicjatywą właścicieli lub użytkowników obiektów tej infrastruktury w kierunku przywracania zdolności w przypadku awarii i zniszczeń. I po ósme – konieczna jest odbudowa sił obrony cywilnej w naszym kraju, niezbędnego elementu ochrony infrastruktury krytycznej oraz ochrony ludności, zarówno w czasie klęsk żywiołowych, jak i kryzysu polityczno - militarnego i wojny. ◄

Materiały źródłowe

[1] Ch. Fjaeder: The nation – state, national security and resilience in the age of globalisation, Resilience Vol. 2, No. 2

[2] Elektrownie w Polsce – Paweł Madejski (agh.edu.pl). pobrano 20.03.2023 r. godz. 17.30

[3] NATO - Official text: Commitment to enhance resilience - Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, 08-Jul.-2016. Pobrano : 20.03.2023 godz. 20.00

[4] NATO - Official text: Strengthened Resilience Commitment (2021), 14-Jun.-2021. Pobrano : 20.03.2023 godz. 20.30

[5] R. Zięba, J. Zając: Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski – Ekspertyza, Warszawa październik 2010

[6] Rozporządzenie Rady Ministrów z dnia 2 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony. Dz. U. 2003 nr 116 poz. 1090

[7] S. Koziej: Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych, Krytyka i Prawo, tom 8, nr 1/2016

[8] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Warszawa 2020

[9] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz. U. 2022 poz. 261, art. 3

[10] W. Walczak: Zarządzanie kryzysowe – rola i zadania organów administracji państwowej. Przedsiębiorczość i Zarządzanie, T.X, zeszyt 8/2009, s. 93

[11] Źródła energii w Polsce w 2020: mniej węgla, więcej gazu i OZE - WysokieNapiecie.pl, pobrano 20 marca 2023 r. godz. 19.00

Drogowe odcinki lotniskowe jako element infrastruktury krytycznej i obronnej państwa

Highway landing strips as an element of critical and defence infrastructure of the country

Mariusz Wesołowski

Dr hab. inż.

Wojskowy Instytut Techniki Pancernej i Samochodowej

mariusz.wesolowski@witpis.eu
ORCID: 0000-0002-5545-8831

Krzysztof Blacha

Dr inż.

Instytut Techniczny Wojsk Lotniczych

krzysztof.blacha@itwl.pl
ORCID: 0000-0002-4599-4294

Adam Poświata

Dr inż.

Instytut Techniczny Wojsk Lotniczych

adam.poswiata@itwl.pl
ORCID: 0000-0002-7861-1616

Streszczenie: Jednym z bardzo istotnych elementów infrastruktury krytycznej i obronnej Polski, obok sieci lotnisk wojskowych i cywilnych, są drogowe odcinki lotniskowe, których funkcja, znaczenie i przydatność nabrały szczególnego wymiaru w aktualnej sytuacji geopolitycznej, w tym przede wszystkim podczas trwającego konfliktu zbrojnego w Ukrainie. Drogowe odcinki lotniskowe (DOL) to specjalnie przygotowane odcinki dróg publicznych przystosowane do wykonywania operacji lotniczych startu i lądowania wojskowych statków powietrznych (WSP) realizujących zadania operacyjne w czasie kryzysu i wojny oraz zadania wynikające z realizacji procesu szkolenia lotniczego. Szczegółowe informacje dotyczące wymagań stawianym DOL przedstawiono w normie obronnej NO-17-A207:2022 Nawierzchnie lotniskowe – Drogowe odcinki lotniskowe – Wymagania i badania [1]. W ww. dokumencie normatywnym określono minimalne wymagania w zakresie wymiarów geometrycznych, obszarów o ograniczonych przeszkodach oraz układów konstrukcyjnych nawierzchni DOL. Przedstawiono wymagania dla podstawowych parametrów eksploatacyjnych nawierzchni na obiektach użytkowanych przez służby drogowe, które należy stosować przede wszystkim: przy projektowaniu i budowie DOL, modernizowaniu i przebudowie istniejących drogowych odcinków lotniskowych, odbiorze wykonanych robót, ocenie technicznej i eksploatacyjnej. Postanowienia normy są właściwe dla oceny stanu technicznego DOL w całym okresie ich technicznej żywotności, a szczególnie w okresie ich użytkowania przez wojskowe statki powietrzne. Stan techniczny i użytkowy nawierzchni DOL ma bezpośredni wpływ na bezpieczeństwo wykonywania operacji lotniczych. Wymusza to konieczność posiadania aktualnej, pełnej wiedzy o ich stanie technicznym, co będzie pozwalało podejmować odpowiednie decyzje mające na celu zapewnienie ich bezpiecznej eksploatacji. W artykule przedstawiono wyniki badań parametrów eksploatacyjnych nowowybudowanych konstrukcji nawierzchni drogowego odcinka lotniskowego Wielbark w ciągu drogi wojewódzkiej nr 604 oraz wymagania obowiązującej normy obronnej NO-17-A207:2022. Omówiono również możliwe zagrożenia eksploatacyjne dla wykonywania operacji lotniczych przez wojskowe statki powietrzne oraz realizowane prace dla poprawy bezpieczeństwa na DOL, wchodzących w skład elementów infrastruktury krytycznej i obronnej państwa.

Słowa kluczowe: *Drogowy odcinek lotniskowy, Infrastruktura krytyczna, Obronność, Bezpieczeństwo, Nawierzchnia lotniskowa*

Abstract: One of the essential elements of the Polish critical and defence infrastructure, apart from the network of military and civil airports, are highway landing strips, which function, importance and usefulness have taken on a special dimension in the current geopolitical situation, especially during the ongoing armed conflict in Ukraine. Highway Landing Strips (Polish. DOL) are specially prepared sections of public roads adapted to perform air operations of take-off and landing of military aircraft (Polish. WSP) intended for operational tasks during crisis and war, as well as tasks resulting from the implementation of the flight training process. Detailed information on the requirements for DOL is presented in NO-17-A207:2022 Airfield pavements – Airfield road strips – Requirements and tests [1]. The above normative document outlines the minimum requirements for geometric dimensions, runway obstacle free zones and DOL surface construction systems. Requirements for the basic operating parameters of pavements on facilities used by road services have been presented. In addition, these requirements should be primarily used in designing and constructing DOL, modernizing and reconstructing the existing road sections of airfields, accepting the performed works, and technical and operational assessment. The normative provisions are appropriate for assessing the technical condition of DOLs throughout their entire technical lifetime, especially during their use by military aircraft. The technical and operational condition of the DOL surface has a direct impact on the safety of air operations. This enforces the need for up-to-date, full knowledge about their technical condition, which will help make the appropriate decisions to ensure their safe operation. The article presents the results of testing the operational parameters of the newly built structures of the surface of the Highway Landing Strip of Wielbark airport along provincial road No. 604 and the requirements of the applicable defence standard NO-17-A207:2022. The possible operational hazards for performing air operations by military aircraft and the ongoing works aimed at improving the security of the DOL, which are part of the critical and defence infrastructure of the country, are also discussed.

Keywords: *Road section of the airport, Critical infrastructure, Defence, Security, Airport pavement*

Wstęp

Jednym z elementów infrastruktury krytycznej systemu obronności i bezpieczeństwa państwa są drogowe odcinki lotniskowe. Koncepcja DOL stała się popularna w okresie powojennym. Pomysł rozwijano równolegle do prac nad samolotami pionowego startu, mogących operować z dowolnego miejsca. Drogowe odcinki lotniskowe stały się popularne w Polsce, Niemczech (zarówno RFN jak i NRD), Szwajcarii, Finlandii, Szwecji, Korei Północnej, Chinach czy Czechosłowacji. Skandynawia nadal prowadzi ćwiczenia z użyciem odcinków autostrad w charakterze tymczasowych baz lotniczych. Finowie posiadając w swoim arsenale samoloty F/A-18 Hornet, czyli maszyny

projektowane jako samoloty pokładowe wyposażone w hak ogonowy mogą skorzystać z systemu lin hamujących skracającego dobieg, co jest niezwykle przydatne w przypadku operacji na improwizowanych pasach. Ćwiczenia w operowaniu ze swoich autostrad prowadzi też Singapur. Amerykanie, szczególnie w ramach doktryny zimnowojennej szkolili swoich pilotów w RFN, a ćwiczenia na niemieckich autostradach odbywały się regularnie nawet w latach 80-tych ubiegłego wieku. Użycie dróg jako lotnisk jest nadal powszechne w Rosji, Pakistanie, w Republice Chińskiej, a obecnie także i w Ukrainie.

W Polsce, ostatnie szkolenie lotnicze na drogowym odcinku lotniskowym odbyło się w roku 2003 na drodze wojewódzkiej nr 142 (DW142) łączącej nowy węzeł drogi ekspresowej S3 z dawną "berlinką" w kierunku Chociwla, na tzw. DOL Kliniska. Na rys. **1** przedstawiono przykłady wykonywania operacji lotniczych startu i lądowania WSP na drogowym odcinku lotniskowym.

W terenie naszego kraju występuje 21 drogowych odcinków lotniskowych. W najlepszym stanie technicznym i eksploatacyjnym znajdują się: wspomniany powyżej DOL Kliniska, DOL Jaźwiny (zlokalizowany na autostradzie A4 pomiędzy węzłami Tarnów Północ, a Dębica Wschód) oraz DOL Września (usytuowany na autostradzie A2 w okolicy Wrześni k. Poznania). Pozostałe drogowe odcinki lotniskowe są w różnym stanie, w większości przypadków nie nadają do użytkowania z uwagi na ich niezadowalający stan techniczny, ale w ostatnim czasie jeden z nich został przebudowany do nowych parametrów technicznych spełniających wymagania normy obronnej [1]. Przedmiotowy drogowy odcinek lotniskowy znajduje się w ciągu drogi wojewódzkiej nr 604 (DW604) na odcinku Robaczewo – Wielbark, tzw. DOL Wielbark. Pas drogowy posiada szerokość 90 m, a w jego skład wchodzą następujące elementy funkcjonalne:

- droga startowa o nawierzchni z betonu cementowego o szerokości 30 m i długości 2440 m,
- 2 boczne pasy bezpieczeństwa o szerokości 30 m po obu stronach drogi startowej i wybiegów,
- 2 wybiegi o nawierzchni z betonu cementowego na przedłużeniu drogi startowej o szerokości 30 m i długości 275 m (jako część czołowych pasów bezpieczeństwa),
- 2 płaszczyzny postoju samolotów o nawierzchni z betonu cementowego i wymiarach 200 m x 45 m, przyległe do końcowych odcinków drogi startowej,
- 2 odcinki przejściowe do przekroju drogowego o nawierzchni z betonu asfaltowego na przedłużeniu wybiegów po 125 m każdy (jako część czołowych pasów bezpieczeństwa).

Wymienione powyżej elementy funkcjonalne DOL Wielbark zostały poddane szczegółowym badaniom odbiorczym w zakresie spełnienia wymagań eksploatacyjnych dedykowanych WSP.

Wymagania dotyczące wymiarów geometrycznych, obszarów o ograniczonych przeszkodach oraz układów konstrukcyjnych nawierzchni DOL zostały szczegółowo przedstawione w normie obronnej NO-17-A207:2022 [1]. Ponadto, omówiono w niej wymagania dla podstawowych parametrów eksploatacyjnych nawierzchni na obiektach użytkowanych przez służby drogowe.

Postanowienia przedmiotowej normy należy stosować przy projektowaniu i budowie drogowych odcinków lotniskowych, modernizowaniu i przebudowie istniejących DOL, odbiorze wykonanych robót, a także ich ocenie technicznej i eksploatacyjnej w całym okresie cyklu życia. W związku z powyższym, DOL muszą spełniać również wymagania określone w innych normach obronnych, które bezpośrednio dotyczą nawierzchni lotniskowych, tj.:

- NO-17-A204:2015 Nawierzchnie lotniskowe – Nawierzchnie z betonu cementowego – Wymagania i metody badań [2],
- NO-17-A200:2017 Nawierzchnie lotniskowe – Nawierzchnie z betonu asfaltowego – Wymagania i badania [3],
- NO-17-A500:2016 Nawierzchnie lotniskowe i drogowe – Badania nośności [4],
- NO-17-A502:2015 Nawierzchnie

a) Start samolotu Su-22

b) Lądowanie samolotu MiG-29

***1**. Szkolenie lotnicze wojskowych statków powietrznych na DOL Kliniska*

lotniskowe – Badania równości [5],
- NO-17-A501:2015 Nawierzchnie lotniskowe – Badania szorstkości [6],
- NO-17-A503:2017 Nawierzchnie lotniskowe – Darniowe i gruntowe nawierzchnie lotniskowe – Badania nośności [7],
- NO-17-A205:2017 Zimowe utrzymanie nawierzchni lotniskowych – Stosowanie środków do odladzania – Wymagania i badania [8].

Na bezpieczeństwo realizacji operacji lotniczych wpływa wiele czynników, które można zgrupować w trzech kategoriach, tj.; człowiek (personel pokładowy, personel utrzymujących zdatność statków powietrznych, personel kierujący ruchem lotniczym, personel obsługujący urządzenia lotniskowe), statek powietrzny (samoloty, śmigłowce i inne obiekty latające) oraz otoczenie (DOL, w tym nawierzchnie lotniskowe oraz przestrzeń powietrzna). Priorytetowym zadaniem służby lotniskowej jest w pierwszej kolejności zapewnienie bezpiecznej eksploatacji nawierzchni lotniskowych przez WSP.

Wymagania dotyczące DOL

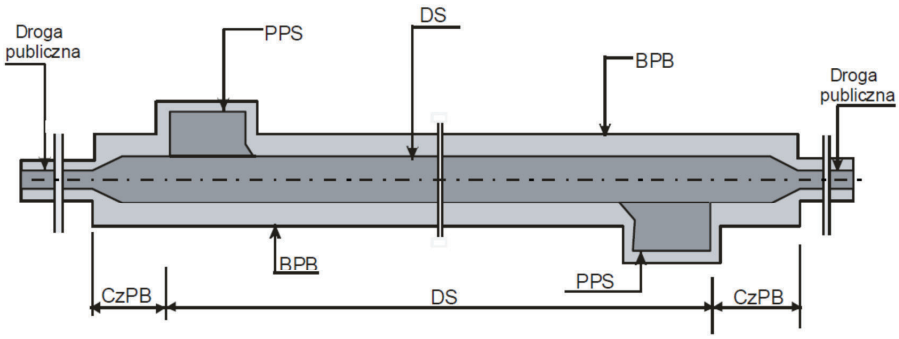
DOL to prosty odcinek drogi o określonych parametrach oraz wymiarach poziomych i pionowych części przestrzeni powietrznej, która jest niezbędna do wykonywania operacji lotniczych. Do usytuowania DOL należy wykorzystywać drogi publiczne [9], posiadające wymaganą długość oraz odpowiednią nośność, zarządzane przez służby drogowe. Układ drogowy powinien umożliwiać objazd DOL przez transport samochodowy (w przypadku czasowego wyłączenia DOL dla ruchu kołowego podczas wykonywania operacji lotniczych). W przypadku lokalizacji DOL w terenie zalesionym, w którym występują zwierzęta mogące mieć wpływ na bezpieczeństwo wykonywania operacji lotniczych przez WSP poprzez wtargnięcie na drogę startową, DOL należy zabezpieczyć (np. ogrodzeniem zewnętrznym).

DOL powinien składać się z niżej wymienionych elementów funkcjonalnych:
- drogi startowej (DS),
- czołowych pasów bezpieczeństwa (CzPB),
- bocznych pasów bezpieczeństwa (BPB),
- płaszczyzn postoju samolotów (PPS),
- dróg kołowania (DK) – w przypadku takiej potrzeby,
- obszarów o ograniczonych przeszkodach.

Rozmieszczenie elementów DOL przedstawiono na rys. **2**. Należy podkreślić, że nawierzchnia płaszczyzny postoju samolotów powinna być wykonana z betonu cementowego spełniającego wymagania [2] oraz spełniać wymagania nośności przyjętej dla drogi startowej.

Wymagania geometryczne

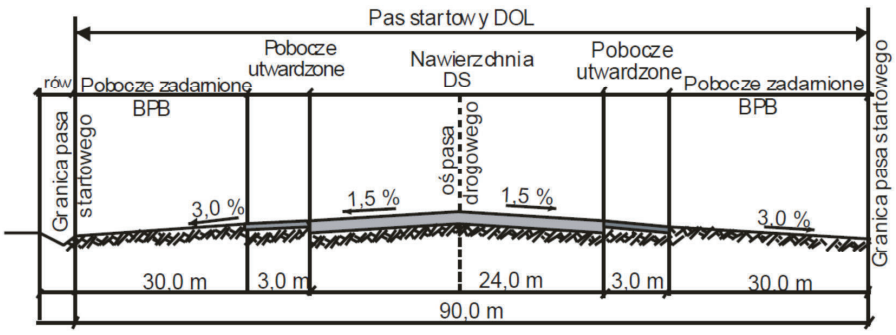
Powierzchnię DOL stanowi prostoliniowy pas drogowy o szerokości 90 m i długości minimum 2990 m, zawarty pomiędzy granicami CzPB. Utrzymanie pasa drogowego według zasad lotniskowych obowiązuje również na odcinkach drogi publicznej poza pasem startowym DOL na odcinku wynoszącym 1000 m, jeśli przebiegają one na powierzchniach podejść powietrznych. Wymagania geometryczne dotyczące wymiarów, spadków oraz łuków pionowych na DS, PPS oraz CzPB i BPB DOL przedstawiono w tablicy **1.** Przekrój poprzeczny DOL przedstawiono przykładowo na rys. **3**, natomiast na rys. **4** pokazano schemat wybiegu oraz BPB i CzPB.



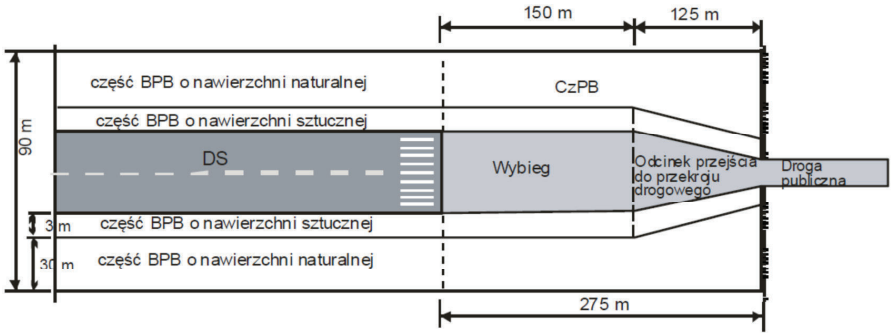
***2**. Elementy drogowego odcinka lotniskowego [1]*

***Tab. 1.** Wymagania geometryczne dla DOL*

Parametr	Wartości
Całkowita długość DOL, w tym: a) długość DS b) długość CzPB c) długość wybiegu	≥ 2990 m ≥ 2440 m ≥ 275 m 150 m
Całkowita szerokość pasa startowego, w tym: a) szerokość DS b) szerokość każdego z BPB, w tym: - część o nawierzchni sztucznej - część o nawierzchni sztucznej	≥ 90 m ≥ 24 m ≥ 33 m ≥ 3 m ≥ 30 m
Pochylenie podłużne nawierzchni	≤ 1,5 %
Pochylenie poprzeczne DS	≥ 0,5 % i ≤ 1,5 %
Pochylenie poprzeczne BPB i CzPB	≤ 3,0 %
Pionowy promień krzywizny powierzchni DS i BPB w kierunku podłużnym	≥ 8000 m
Długość PPS	≥ 200 m
Szerokość PPS	≥ 45 m
Szerokość DK	≥ 15 m



***3**. Przekrój poprzeczny pasa startowego DOL [1]*



***4**. Wymiary geometryczne wybiegu oraz BPB i CzPB DOL [1]*

Na DOL będzie głównie odbywał się ruch samochodowy, dlatego etap projektowania lub adaptacji tych odcinków powinien uwzględniać rozwiązania i wymagania drogowe (np. wymagania konstrukcyjne). Zasady projektowania i wymagania techniczne dla DOL dotyczą natomiast głównie warstwy jezdnej oraz poboczy i stref bezpieczeństwa. Na całej długości pasa startowego DOL nie mogą się znajdować żadne budowle naziemne i podziemne oraz jakiekolwiek przeszkody (drzewa, znaki, skarpy, ekrany, itp.) z wyjątkiem istniejących drogowych przepustów odwadniających z wlotami i wylotami usytuowanymi poza pasem drogowym. W przypadku ustawienia elementów stanowiących przeszkody (np. bariery rozdzielające ruch), muszą być one łatwe w demontażu i usuwaniu. W pasie startowym DOL oraz w obszarach o ograniczonych przeszkodach oznakowania pionowe należy ograniczyć do niezbędnego minimum, z możliwością ich szybkiego zdemontowania. Ponadto, w pasie startowym DOL wyklucza się skrzyżowania i połączenia z innymi drogami, dopuszcza się natomiast zjazdy gruntowe do celów gospodarczych, lecz bez przepustów drogowych.

Przejście z jednego pochylenia podłużnego DS do drugiego należy wykonać płaszczyzną zakrzywioną, której stopień zmiany pochylenia nie powinien przekraczać 0,1 % na 30 m. Płynność łączenia sąsiednich odcinków DS o różnych pochyleniach podłużnych należy zapewnić poprzez zachowanie dopuszczalnych krzywizn powierzchni w płaszczyźnie pionowej. Minimalny promień tej krzywizny powinien wynosić 8000 m. Jeżeli nie można uniknąć zmian pochylenia DS, to zmiany te należy wykonać, zapewniając linię widoczności, tak żeby każdy punkt usytuowany na wysokości 3 m nad DS był widoczny z każdego innego punktu usytuowanego również 3 m nad DS w odległości równej co najmniej połowie długości DS. W celu zapewnienia możliwie jak najszybszego odprowadzenia wody, nawierzchnia DS powinna być dwuspadowa, pochylenie po obu stronach osi powinno być symetryczne. Pochylenie poprzeczne powinno być w przybliżeniu jednakowe na całej długości DS, gdzie należy zapewnić płynne przejście spadków, ze względu na konieczność zapewnienia dobrego spływu wody.

Nawierzchnia poboczy DS powinna być wysokościowo zrównana z nawierzchnią DS, natomiast pochylenie poprzeczne poboczy nie powinno przekraczać 3,0 %. W przypadku utrudnień w odprowadzeniu wody powierzchniowej z BPB, powierzchnie te mogą być zakończone rowami trójkątnymi o łagodnych skarpach nie mniejszych niż 1:5 i przeciwskarpach 1:2. Rowy nie powinny przekraczać głębokości 1,0 m i nie mogą być usytuowane w obszarze pasa drogowego.

PPS powinny być zlokalizowane w odległości minimum 50 m od zewnętrznych granic DS. Minimalne wymiary PPS to: długość 200 m, a szerokość 45 m (od krawędzi DS).

W przypadku lokalizacji DOL w pasie autostrady, gdzie na PPS będą wykorzystywane miejsca obsługi pasażerów, które są oddzielone od DS np. pasem zieleni, płaszczyzny takie należy połączyć z DS drogami kołowania, zapewniającymi dojazd do nich oraz wykołowanie na DS o minimalnej szerokości 15 m. Szerokość PPS w takim przypadku określa się od krawędzi pasa zieleni. Pochylenie PPS na stanowiskach dla WSP oraz DK powinno zapobiegać gromadzeniu się wody na wymienionych elementach funkcjonalnych DOL. PPS powinna być ułożona poziomo na tyle, na ile pozwalają na to warunki odwodnienia. Pochylenie poprzeczne PPS nie powinno przekraczać 2,5 %. Pobocza PPS powinny mieć szerokość wynoszącą minimum 5 m. Pochylenia podłużne poboczy powinny być zgodne z pochyleniami PPS, maksymalne pochylenia poprzeczne nie powinny przekraczać 3,0 %, a minimalne pochylenia powinny zapewnić odprowadzenie wód opadowych.

DK muszą posiadać sztuczną nawierzchnię spełniającą wymagania

nośności przyjętej dla DS.

Promień łuku DK nie powinien być mniejszy niż: na skrzyżowaniu z DS 30 m, a na skrzyżowaniu z PPS 10 m. Pochylenia podłużne nawierzchni DK nie powinny przekraczać 2,5 %, natomiast pochylenia poprzeczne powinny mieścić się w zakresie od 1,0 % do 2,5 %.

W przypadku, gdy PPS są oddzielone od DS np. pasem zieleni, to od każdej PPS powinny być wybudowane dwie DK – jedna umożliwiająca wkołowanie z DS na PPS, a druga umożliwiająca wykołowanie z PPS na DS.

Wymagania konstrukcyjne

Nawierzchnie DOL mogą stanowić układ konstrukcji nawierzchni podatnych, sztywnych, lub złożonych. Należy podkreślić, że DOL użytkowane są przede wszystkim przez pojazdy samochodowe, a ich eksploatacja przez WSP jest doraźna, dlatego rodzaj i układ konstrukcji muszą spełnić wymagania dla nawierzchni przeznaczonej dla ruchu pojazdów samochodowych. Zasady projektowania i wymagania techniczne dla DOL dotyczą głównie warstwy jezdnej, zatem podstawą do projektowania lub adaptacji dróg dla przewidywanego ruchu, tj. transportu samochodowego oraz operacji lotniczych WSP są wymagania przedstawione w Katalogu typowych konstrukcji nawierzchni sztywnych, załącznik do zarządzenia nr 30 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 16 czerwca 2014 r. [10] oraz Katalogu typowych konstrukcji nawierzchni podatnych i półsztywnych, załącznik do zarządzenia nr 31 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 16 czerwca 2014 r. [11].

W przypadku przyjęcia rozwiązań dla układu warstw konstrukcyjnych nawierzchni DOL według wymienionych powyżej katalogów typowych konstrukcji, należy przyjąć układ konstrukcyjny dla kategorii ruchu przynajmniej KR 4. Dopuszcza się indywidualne projektowanie konstrukcji nawierzchni oraz warstwy ulepszonego podłoża w sytuacjach nietypowych pod warunkiem akceptacji przez zarządcę drogi. Rozwiązania innowacyjne niezawarte w ww. katalogach mogą być dopuszczone do stosowania w praktyce po szczegółowej ocenie technicznej. Materiały użyte do budowy warstwy jezdnej nawierzchni sztywnych lub podatnych DOL muszą spełniać wymagania określone w [2] dla nawierzchni sztywnych lub [3] dla nawierzchni podatnych. Warstwa jezdna, zarówno DS, PPS jak i DK nie powinna mieć uszkodzeń zagrażających bezpieczeństwu wykonywania operacji startów i lądowań WSP.

DOL w przekroju poprzecznym powinien mieć symetryczne pochylenia nawierzchni w stosunku do osi DS, zgodne z wymaganiami przedstawionymi w tabeli **1** i na rys. **3**, o szerokości całkowitej minimum 90 m. Szerokość DS o nawierzchni z betonu cementowego lub betonu asfaltowego powinna wynosić nie mniej niż 24 m. Ponadto, pobocza utwardzone przy DS o minimalnej szerokości 3 m powinny posiadać nawierzchnię sztuczną np. z betonu asfaltowego lub cementowego, ułożoną na odpowiedniej podbudowie, umożliwiającą przeniesienie obciążeń pojazdów zabezpieczających bezpieczną eksploatację o każdej porze roku. Poza poboczami utwardzonymi należy przewidzieć BPB, symetrycznie usytuowane wzdłuż DS, przylegające do poboczy utwardzonych o szerokości minimum po 30 m,
o nawierzchni naturalnej (zadarnionej nawierzchni gruntowej). Wybiegi oraz odcinki przejścia do przekroju drogowego powinny posiadać konstrukcje spełniające przyjęte wymagania nośności i wymagania eksploatacyjne dla DS.

Sumaryczna grubość warstw konstrukcyjnych nawierzchni DOL wraz z podłożem gruntowym powinna zabezpieczyć układ konstrukcyjny przed skutkami przemarzania i spełnić wymagania przedstawione w [2]. Liczba i rodzaj warstw występujących w danej konstrukcji nawierzchni zależy od warunków gruntowo-wodnych, kategorii ruchu, specyficznych warunków klimatycznych oraz od materiałów użytych do warstw nawierzchni.

DOL o konstrukcji sztywnej powinien posiadać warstwę jezdną wykonaną z betonu cementowego, która w zależności od kategorii ruchu może być ułożona jako niedyblowana, dyblowana i kotwiona lub zbrojona, zgodnie z wymaganiami podanymi w [2]. Grubość warstwy jezdnej w postaci płyty swobodnej, która nie współpracuje z płytami sąsiednimi i nie jest zbrojona lub pozbawiona innych elementów wzmacniających, nie powinna być mniejsza niż 0,22 m. W uzasadnionych przypadkach, dla zapewnienia współpracy płyt, zaleca się ich łączenie np. na pióro i wpust lub z wykorzystaniem dybli i kotew. W przypadku przewidywanego zastosowania połączeń płyt za pomocą dybli, minimalna grubość warstwy jezdnej powinna wynosić 0,26 m. Dolne warstwy konstrukcji nawierzchni (warstwa podbudowy pomocniczej oraz warstwa mrozoochronna) stanowią fundament dla warstwy górnej konstrukcji nawierzchni. Warstwy te dobierane są w zależności od grupy nośności podłoża gruntowego i od wymaganej nośności dolnych warstw konstrukcji nawierzchni. Właściwe wypełnianie funkcji przez warstwę ulepszonego podłoża oraz przez dolne warstwy konstrukcji nawierzchni zależy od prawidłowego zaprojektowania i wykonania robót ziemnych oraz związanych z nimi elementów odwodnienia wgłębnego i powierzchniowego.

Natomiast w przypadku DOL o konstrukcji podatnej, rodzaj i układ

warstw uzależniony jest od kategorii ruchu występującego i prognozowanego w miejscu jego usytuowania. Rodzaj konstrukcji przyjmuje się na podstawie założeń podanych w [3] i [10] lub na podstawie innych rozwiązań uzgodnionych pomiędzy zainteresowanymi stronami. Podczas projektowania konstrukcji DOL należy uwzględniać miejscowe warunki eksploatacyjno-ruchowe. Do produkcji mieszanki mineralno-asfaltowej należy stosować materiały spełniające wymagania [3]. Minimalna grubość warstwy ścieralnej powinna wynosić 50 mm.

Wymagania w zakresie nośności

Konstrukcja nawierzchni DOL powinna zapewnić bezpieczne wykonywanie operacji lotniczych WSP zarówno lotnictwa taktycznego, jak i transportowego. Dla DOL przyjęto obliczeniowy statek powietrzny, dla którego wymagany jest wskaźnik nośności nawierzchni (sztucznych) – PCN ≥ 35. Przyjęty wskaźnik nośności dotyczy DS, PPS, DK oraz wybiegów i odcinków przejściowych do przekroju drogowego. Nośność konstrukcji nawierzchni DOL
w postaci liczby klasyfikacyjnej nawierzchni PCN (ang. Pavement Classification Number) należy określić metodą ACN-PCN (ang. Aircraft Classification Number - Pavement Classification Number), zgodnie z [4], Załącznikiem 14 ICAO do Konwencji o międzynarodowym lotnictwie cywilnym [12] oraz Aerodrome Design Manual Part 3, Pavements [13]. Kontrolne badania nośności nawierzchni DOL należy przeprowadzać okresowo z częstotliwością od 3 do 5 lat. Pomiary ugięć sprężystych należy wykonywać w okresie wiosennym i/lub w okresie jesiennym zgodnie z wymaganiami określonymi w [4].

awierzchnie naturalne (darniowe i gruntowe) BPB i CzPB eksploatowane w obszarze DOL także należy poddawać kompleksowej ocenie nośności, zgodnie z [7]. Kontrolne badania nośności nawierzchni naturalnych należy wykonać po wybudowaniu DOL oraz przeprowadzać na użytkowanych i/lub będących przedmiotem wymiany darniowych i gruntowych nawierzchniach DOL okresowo, z częstotliwością od 3 do 5 lat. Badania powinny obejmować:

- badanie wytrzymałości warstwy darniowej do głębokości 0,3 m poniżej poziomu terenu,
- badanie nośności nawierzchni naturalnej do głębokości 0,85 m poniżej poziomu terenu.

Badania terenowe nośności naturalnych nawierzchni DOL należy wykonać zgodnie z metodyką przedstawioną w [7] do głębokości 0,85 m poniżej poziomu terenu, dla trzech wydzielonych warstw przedstawionych na rys. **5**, na którym 1 – warstwa pierwsza do głębokości 0,15 m, 2 – warstwa druga od głębokości 0,15 m do głębokości 0,50 m, 3 – warstwa trzecia od głębokości 0,50 m do głębokości 0,85 m.

Pomiary terenowe należy wykonywać w okresie wiosennym, tj. w najbardziej niekorzystnych warunkach gruntowo-wodnych [14]. Dopuszcza się wykonywanie pomiarów terenowych w okresie jesiennym. Nośność naturalnych nawierzchni lotniskowych wyraża się wskaźnikiem CBR (ang. California Bearing Ratio), który oblicza się zgodnie ze wzorem:

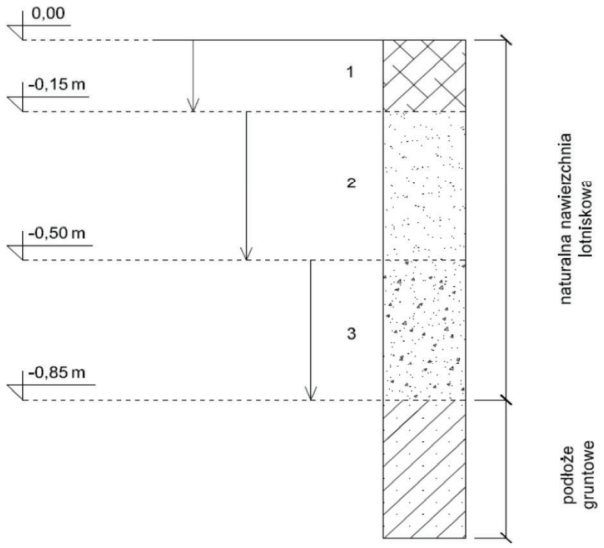
$$CBR = 292 / DCP^{1,12} \quad (1)$$

gdzie: *CBR* – kalifornijski wskaźnik nośności [%], *DCP* – zagłębienie stożka sondy przypadające na jedno uderzenie [mm].

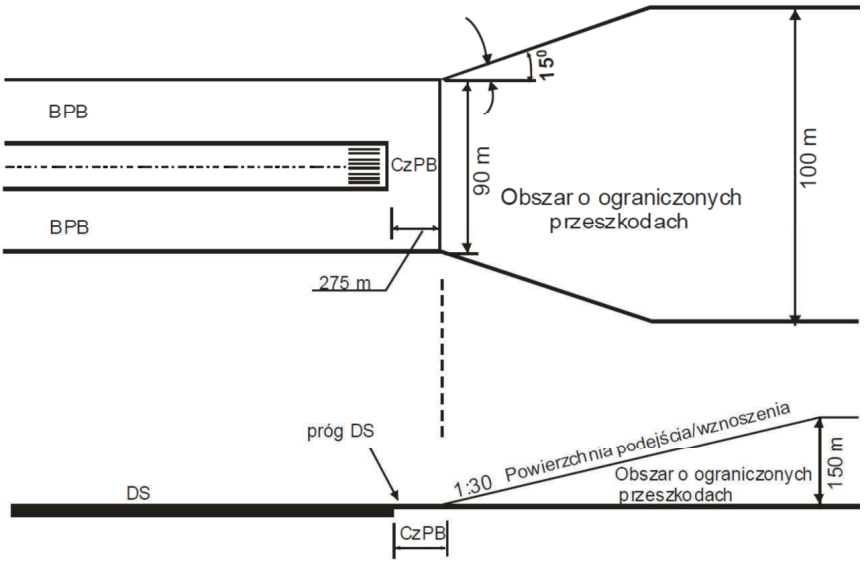
Minimalna wartość CBR powinna wynosić 15 % dla pierwszej warstwy (do głębokości 0,15 m) oraz 8 % dla warstwy powstałej z połączenia warstwy drugiej i trzeciej (od głębokości 0,15 m do głębokości 0,85 m poniżej poziomu terenu). Nawierzchnie naturalne, które nie spełniają wymagań w zakresie nośności, należy poddać działaniom naprawczym, np. doziarnieniu, zagęszczeniu, zabiegom agrotechnicznym lub zabiegom wzmacniającym, np. z zastosowaniem geosyntetyków [15].

Wymagania w zakresie strefy podejść powietrznych

Powierzchnie podejścia/wznoszenia zaczynają się od końców CzPB (275 m za progiem DS), pochylone są w stosunku 1:30 do poziomu DS i wznoszą się na wysokość 150 m. Powierzchnie takie mają szerokość początkową równą szerokości roboczego pasa startowego (90 m), następnie rozszerzają się na zewnątrz pod kątem 15° do szerokości wyno-



***5**. Układ wydzielonych warstw nawierzchni naturalnej w badaniach nośności [7]*



***6**. Powierzchnia podejścia/wznoszenia dla DOL [1]*

szącej 100 m. Powierzchnie podejścia/wznoszenia znajdują się na obu końcach CzPB drogowego odcinka lotniskowego. W strefach takich nie mogą się znajdować żadne przeszkody przekraczające wysokość powierzchni podejścia/wznoszenia. Schemat przedmiotowych powierzchni przedstawiono na rys. **6**. Obiekty wznoszone poza powierzchniami podejścia/wznoszenia muszą zostać uzgodnione z właściwym organem wojskowym, w celu potwierdzenia braku negatywnego wpływu takiego obiektu na operacje lotnicze.

Parametry eksploatacyjne DOL

DOL powinien zapewnić bezpieczne wykonywanie operacji lotniczych przez WSP. W związku z tym, eksploatowana nawierzchnia DOL powinna spełniać określone wymagania w zakresie nośności, równości i szorstkości. Ponadto, w przypadku eksploatacji nawierzchni sztucznych DOL przez WSP w okresie jesienno-zimowym, należy stosować środki odladzające zgodnie z wymaganiami określonymi w [8].

Nośność

Nośność konstrukcji nawierzchni DOL powinna spełniać wymagania określone w projekcie technicznym. Wymagany wskaźnik nośności nawierzchni drogowego odcinka lotniskowego to PCN ≥ 35. Przyjęty wskaźnik dotyczy DS, PPS, wybiegów, odcinków przejścia do przekroju drogowego oraz DK. Ocenę nośności nawierzchni DOL należy prowadzić metodą nieniszczących obciążeń dynamicznych. Ocenę nośności należy przeprowadzić według zasad metody ACN-PCN wymaganą przez ICAO, zgodnie z [4].

W metodzie tej uwzględnia się: rodzaj nawierzchni lotniskowej, kategorię podłoża, maksymalne ciśnienie w oponach statku powietrznego i sposób określenia jej nośności. Do badania nośności nawierzchni lotniskowych stosuje się ciężki ugięciomierz udarowy typu HWD (ang. Heavy Weight Deflectometer). W ramach badań wykonuje się pomiary ugięć sprężystych nawierzchni, na podstawie których wyznacza się wartość wskaźnika nośności PCN i/lub dopuszczalną liczbę operacji lotniczych dla przyjętego typu samolotu obliczeniowego.

W celu przeprowadzenia pełnej analizy nośności ocenianej nawierzchni DOL wykonuje się identyfikację jej konstrukcji poprzez pobranie próbek w postaci odwiertów rdzeniowych, które następnie poddawane są badaniom wytrzymałościowym w warunkach laboratoryjnych [16]. Wyniki uzyskane podczas badania nośności metodą ACN-PCN można przedstawić w postaci wskaźnika nośności PCN i/lub wyznaczonej dopuszczalnej, całkowitej liczby operacji lotniczych, które wyznacza się dla określonej liczby powtórzeń N. Liczba dopuszczalnych powtórzeń obliczana jest w zależności od przyjętego modelu obliczeniowego ocenianej konstrukcji nawierzchni lotniskowej. Dla nawierzchni sztywnych, wykonanych z betonu cementowego, stosuje się następującą formułę wynikającą z kryterium dopuszczalnych naprężeń:

$$N = \left[\frac{R_{zg}}{\sigma} \times \left(\frac{E}{30000}\right)^{1.3}\right]^{(-1/-0.233)} \times 10 \quad (2)$$

gdzie: *Rzg* – wytrzymałość betonu na rozciąganie przy zginaniu [MPa], *σ* – naprężenia rozciągające przy zginaniu wyznaczone w dolnej części płyty betonowej [MPa], *E* – moduł sprężystości betonu [MPa].

Weryfikacja, czy WSP może bezpiecznie wykonywać operacje na danym DOL, sprowadza się do porównania liczby PCN nawierzchni z liczbą ACN samolotu i sprawdzenie warunku ACN ≤ PCN.

Równość

Równość nawierzchni DOL powinna spełniać kryteria podane w [5]. Pomiar równości należy wykonywać zgodnie z metodyką podaną w [5], z wykorzystaniem zmodernizowanego planografu P-3z. Stan równości decyduje nie tylko o komforcie ruchu po nawierzchni DOL, lecz również ma wpływ na wielkość dynamicznych oddziaływań na nawierzchnię [17]. Uzyskanie wymaganej równości to także warunek skutecznego i szybkiego odprowadzenia wód opadowych z nawierzchni DOL. Nawet na niewielkich nierównościach nawierzchni mogą się tworzyć zasto-

iska wody, które w okresie zimowym pogarszają warunki bezpieczeństwa ruchu.

Równość nawierzchni lotniskowych powinna spełniać kryteria określone poziomem wadliwości [18]. Wadliwość rozumiana jest jako procentowa miara ilości przekroczeń nierówności przyjętych w normie jako dopuszczalne. Zgodnie z wyżej wymienioną normą, na podstawie kryterium wadliwości W (%) – przyjmuje się następujące oceny:

- bardzo dobry - $W \leq 5$ %,
- dobry - 5 % $< W \leq$ 10 %,
- dostateczny - 10 % $< W \leq$ 20 %,
- niezadowalający - 20 % $< W \leq$ 50 %,
- niedostateczny - $W >$ 50 %.

Wynik pomiaru stanu równości nawierzchni DOL uznaje się za pozytywny, jeżeli liczba odcinków 5 m trasy pomiarowej przekraczająca dopuszczalne nierówności jest mniejsza niż 20 % dla nawierzchni nowobudowanych lub po remoncie oraz mniejsza od 50 % dla nawierzchni będących w eksploatacji. Zgodnie z wymaganiami zawartymi w [5] dopuszczalne nierówności dla nowobudowanych nawierzchni DOL oraz maksymalne wartości nierówności dla nawierzchni eksploatowanych powinny spełniać kryteria przedstawione w tabeli **2**.

Szorstkość

Szorstkość nawierzchni DOL powinna spełniać kryteria dla nawierzchni lotniskowych podane w [6]. Stan szorstkości nawierzchni ma niezwykle istotne znaczenie dla bezpieczeństwa wykonywania operacji lotniczych. Badania szorstkości nawierzchni DOL wykonuje się zgodnie z wymaganiami: normy obronnej [6], Załącznika 14 ICAO do Konwencji o Międzynarodowym Lotnictwie Cywilnym [12] oraz Advisory Circular No: 150/5320-12C Measurement, Construction, and Maintenance of Skid Resistant Airport Pavement Surfaces Document Information, FAA, 1997 [19]. W normie [6] omówiono metodykę badania szorstkości nawierzchni lotniskowych, określono wymagania dotyczące aparatury stosowanej do pomiarów w warunkach terenowych oraz przedstawiono kryteria oceny stanu szorstkości nawierzchni lotniskowych (wartości średnie wymaganych współczynników tarcia) w zależności od zastosowanego typu urządzenia pomiarowego i warunków pomiaru (prędkość pomiaru, typ opony pomiarowej, pomiar z wodą lub bez wody).

Tab. 2. *Maksymalne i dopuszczalne nierówności dla nawierzchni DOL*

Rodzaj urządzenia	Maksymalne nierówności	Dopuszczalne nierówności
Planograf lub łata 4 m	12 mm	5 mm
Planograf lub łata 3 m	9 mm	3 mm

Współczynnik tarcia jest podstawowym parametrem charakteryzującym nawierzchnię lotniskową pod względem szorstkości [20]. Tarcie jest zjawiskiem występującym na styku powierzchni ciał materialnych. Siła tarcia zależy od dwóch parametrów, tj.: wartości siły nacisku jednego ciała na drugie oraz współczynnika tarcia. W przypadku tarcia statycznego, kiedy obiekty pozostają nieruchome względem siebie, współczynnik tarcia jest stały. Ogólny wzór na maksymalną siłę tarcia ma postać:

$$T = \mu N \qquad (3)$$

gdzie: T – wartość siły tarcia [N], μ – wartość współczynnika tarcia [-], N – wartość siły nacisku jednego obiektu na drugi [N].

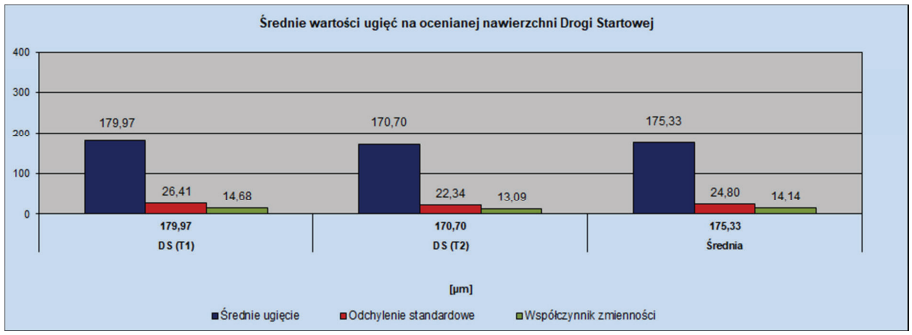
Wymagane, średnie wartości współczynników tarcia określono dla trzech przedziałów, tj.: dla projektowanych, nowych nawierzchni lotniskowych, dla użytkowanych i/lub będących przedmiotem planowania prac remontowych oraz minimalne (graniczne). Badania szorstkości nawierzchni DOL należy wykonywać urządzeniami umożliwiającymi ciągły pomiar współczynnika tarcia między kołem poruszającego się statku powietrznego a nawierzchnią lotniskową. Należy stosować urządzenia z oponą gładko bieżnikowaną, wyposażone w układ samozraszający, umożliwiający pomiar współczynnika tarcia nawierzchni lotniskowej pokrytej warstwą wody o grubości nie mniejszej niż 1 mm przy dwóch prędkościach pomiarowych, tj. 65 km/h lub 95 km/h. Przykładowo, wymagane wartości współczynnika tarcia dla nawierzchni lotniskowych poddanych ocenie przy wykorzystaniu urządzenia pomiarowego w postaci testera tarcia ASFT (ang. Airport Surface Friction Tester) na przyczepie T-10 przy prędkości pomiaru 65 km/h przedstawiają się następująco:

- dla projektowanych, nowych nawierzchni lotniskowych – 0,70,
- dla użytkowanych i/lub będących przedmiotem planowania prac remontowych – 0,50,
- minimalna (graniczna) – 0,40.

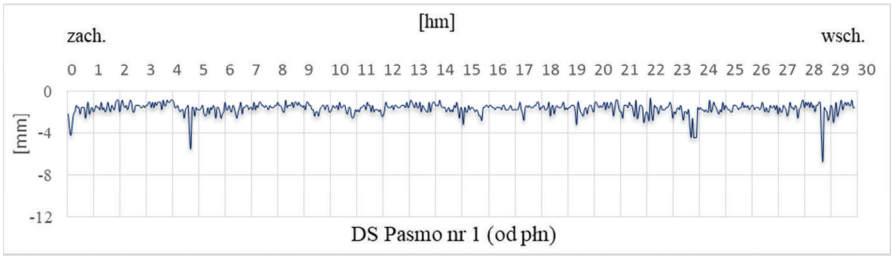
Wyniki badań dla DOL Wielbark

W ramach realizowanej inwestycji pn. Rozbudowa drogi wojewódzkiej nr 604 na odcinku Robaczewo – Wielbark przeprowadzono badania odbiorcze, które obejmowały określenie parametrów eksploatacyjnych nawierzchni DOL w zakresie nośności, równości oraz szorstkości. Elementami funkcjonalnymi ocenianego DOL Wielbark były: droga startowa z betonu cementowego o szerokości 30 m i długości 2440 m (sumaryczna długość wraz z wybiegami 2990 m) oraz dwie płaszczyzny postoju samolotów (PPS EAST i PPS WEST) także o nawierzchni z betonu cementowego i wymiarach 200 m x 45 m. W artykule przedstawiono wyniki z przeprowadzonych badań, ale tylko w odniesieniu do DS.

Badanie nośności zostało przeprowadzone z wykorzystaniem ugię-



***7**. Zestawienie wartości ugięć sprężystych dla konstrukcji nawierzchni DS [21]*



***8**. Profil nierówności podłużnych na trasie pomiarowej nr 1 – pasmo nr 1 (DS) [21]*

ciomierza lotniskowego typu HWD zgodnie z wymaganiami normy obronnej [4]. W wyniku wykonanej analizy nośności określono całkowite, dopuszczalne liczby operacji lotniczych dla ocenianych elementów funkcjonalnych DOL, uwzględniając przyjęty w dokumentacji projektowej wskaźnik nośności PCN 35. Uzyskane wyniki podczas pomiarów terenowych, w postaci wykresu średnich wartości ugięć sprężystych dla badanej konstrukcji nawierzchni DS, przedstawiono na rys. **7** [21]. Natomiast wyznaczona, całkowita, dopuszczalna liczba operacji lotniczych N wyniosła 125 000 dla wskaźnika PCN 35/R/B/W/T.

Badanie równości ocenianych nawierzchni DOL Wielbark przeprowadzono z wykorzystaniem zmodernizowanego planografu typu P-3z, zgodnie z normą obronną [5]. Ocenę stanu równości nawierzchni przeprowadzono na podstawie kryterium wadliwości W. Uzyskane wyniki podczas pomiarów terenowych (dla DS), w postaci profilu nierówności podłużnych dla jednej z tras przedstawiono na rys. **8**. Natomiast wyznaczone wartości wadliwości W wyniosły odpowiednio: 0,9 % w kierunku podłużnym (stan bardzo dobry) oraz 16,4 % w kierunku poprzecznym (stan dostateczny) [21].

Pomiary w zakresie szorstkości realizowane były zgodnie z metodyką określoną w normie obronnej [6]. W wyniku przeprowadzonych pomiarów, określono aktualne (na dzień przeprowadzenia badań) wartości współczynnika tarcia dla ocenianych nawierzchni DOL Wielbark. Uzyskane wyniki podczas pomiarów terenowych (dla DS), w postaci średnich wartości współczynnika tarcia μ przedstawiono w tabeli **3** [21].

Na podstawie wykonanych badań odbiorczych nawierzchni DS na DOL Wielbark w zakresie nośności, równości i szorstkości, można sformułować następujące wnioski:

1. Przeprowadzone badania polowe z wykorzystaniem ugięciomierza udarowego typu HWD wykazały, że podłoże gruntowe występujące pod badaną konstrukcją nawierzchni DS,

w momencie jego badania, można ocenić jako grunty o średniej kategorii nośności.

2. Konstrukcja ocenianej nawierzchni DS spełniła wymagania w zakresie nośności dla przyjętego wskaźnika PCN 35.
3. Oceniana nawierzchnia DS spełniła wymagania w zakresie równości, określone dla nowych nawierzchni lotniskowych w normie obronnej [5].
4. Podlegająca ocenie nawierzchnia DS spełniła także wymagania w zakresie szorstkości, określone w [6] dla nowych nawierzchni lotniskowych.

Podsumowanie

Drogowe odcinki lotniskowe obok sieci lotnisk cywilnych, wojskowych i aeroklubowych, to aktualnie jeden z bardzo ważnych elementów infrastruktury krytycznej i obronnej naszego państwa. Ich rola, zadania, znaczenie i przydatność nabrały szczególnego wymiaru w aktualnej sytuacji geopolitycznej, tj. podczas trwającego konfliktu zbrojnego w Ukrainie.

DOL to specjalnie przygotowane odcinki dróg publicznych przystosowane do wykonywania operacji lotniczych startu i lądowania wojskowych statków powietrznych realizujących zadania operacyjne w czasie kryzysu i wojny jak również zadania wynikające z realizacji procesu szkolenia lotniczego. DOL to proste odcinki dróg o określonych parametrach oraz wymiarach poziomych i pionowych części przestrzeni powietrznej, które obejmują: drogę startową, płaszczyzny postoju samolotów, drogi kołowania (jeśli są one konieczne), boczne pasy bezpieczeństwa, czołowe pasy bezpieczeństwa oraz obszary o ograniczonych przeszkodach. Do właściwego

***Tab. 3.** Wyniki pomiarów współczynnika tarcia dla nawierzchni DS na DOL Wielbark*

EFL	Trasa pomiarowa	Wartość minimalna współczynnika tarcia	Wartość maksymalna współczynnika tarcia	Wartość średnia współczynnika tarcia
DS	1	0,54	0,84	0,71
	2	0,53	0,88	0,72
			Średnia:	0,72

usytuowania DOL należy wykorzystywać drogi publiczne zarządzane przez służby drogowe, posiadające wymaganą długość oraz odpowiednią nośność.

W artykule przedstawiono wymagania geometryczne, konstrukcyjne, w zakresie nośności i stref podejść powietrznych stawiane DOL, które szczegółowo określa obowiązująca norma obronna NO-17-A207:2022. Omówiono także wymagania dla podstawowych parametrów eksploatacyjnych nawierzchni na obiektach użytkowanych przez służby drogowe, które należy stosować przede wszystkim: przy projektowaniu i budowie DOL, modernizowaniu i przebudowie istniejących drogowych odcinków lotniskowych, odbiorze wykonanych robót, ocenie technicznej i eksploatacyjnej. Należy podkreślić, że postanowienia ww. normy są właściwe dla oceny stanu technicznego DOL w całym okresie ich technicznej żywotności, a szczególnie w okresie ich użytkowania przez wojskowe statki powietrzne.

Ponadto, w artykule zaprezentowano uzyskane wyniki badań parametrów eksploatacyjnych nowowybudowanej konstrukcji nawierzchni drogi startowej DOL Wielbark w ciągu drogi wojewódzkiej nr 604. Na podstawie uzyskanych wyników badań w zakresie nośności, równości i szorstkości stwierdzono, że oceniana konstrukcja nawierzchni DS spełniła wszystkie wymagania normowe oraz założenia projektowe i może zostać dopuszczona do eksploatacji. ◄

Materiały źródłowe

[1] NO-17-A207:2022 Nawierzchnie lotniskowe – Drogowe odcinki lotniskowe – Wymagania i badania.

[2] NO-17-A204:2015 Nawierzchnie lotniskowe – Nawierzchnie z betonu cementowego – Wymagania i metody badan.

[3] NO-17-A200:2017 Nawierzchnie lotniskowe – Nawierzchnie z betonu asfaltowego – Wymagania i badania.

[4] NO-17-A500:2016 Nawierzchnie lotniskowe i drogowe – Badania nośności.

[5] NO-17-A502:2015 Nawierzchnie lotniskowe – Badania równości.

[6] NO-17-A501:2015 Nawierzchnie lotniskowe – Badania szorstkości.

[7] NO-17-A503:2017 Nawierzchnie lotniskowe – Darniowe i gruntowe nawierzchnie lotniskowe – Badania nośności.

[8] NO-17-A205:2017 Zimowe utrzymanie nawierzchni lotniskowych – Stosowanie środków do odladzania – Wymagania i badania.

[9] Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz.U. z 2020 r. poz. 470,
z późn. zm.).

[10] Katalog typowych konstrukcji nawierzchni sztywnych, załącznik do zarządzenia nr 30 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 16 czerwca 2014 r.

[11] Katalog typowych konstrukcji nawierzchni podatnych i półsztywnych, załącznik do zarządzenia nr 31 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 16 czerwca 2014 r.

[12] Załącznik 14 ICAO do Konwencji o międzynarodowym lotnictwie cywilnym, Lotniska Tom I – Projektowanie i eksploatacja lotnisk, wydanie 11, styczeń 2019.

[13] Aerodrome Design Manual Part 3, Pavements, ICAO, Doc-9157-AN/901.

[14] Wesołowski M., Pietruszewski P., Iwanowski P. Analysis of natural airfield pavement load-bearing capacity in the aspect of air operation safety. „Proceedings of the 29th European Safety and Reliability Conference", Beer, M., Zio, E. Ed., Research Publishing, Singapore, 2019.

[15] Wesołowski M., Kowalewska A. The impact of a geogrid system on load-bearing capacity of natural airfield pavements. Archives of Civil Engineering, 2020, Vol. LXVI, 52, nr DOI: 10.24425/ace.2020.131795

[16] Wesołowski M., Blacha K. The Impact of Load Bearing Capacity of Airfield Pavement Structures on the Air Traffic Safety. "Environmental Engineering", 10th International Conference, Litwa, 27-28 Kwietnia 2017.

[17] Poświata A., Pietruszewski P., Włodarski P. Wpływ nierówności nawierzchni lotniskowych na stan techniczny i bezpieczeństwo operacji lotniczych. Przegląd Komunikacyjny 2022, nr 10, 11-17.

[18] Pietruszewski P., Poświata A., Wesołowski M. Evaluation of airfield pavement evenness. IOP Conf. Series: Materials Science and Engineering, 2018.

[19] Advisory Circular No: 150/5320-12C Measurement, Construction, and Maintenance of Skid Resistant Airport Pavement Surfaces Document Information, FAA, 1997.

[20] Wesołowski M., Blacha K. Evaluation of airfield pavement micro and macrotexture in the light of skid resistance (friction coefficient) measurements. MATEC Web of Conferences, Volume 262, (05017), 2019.

[21] Wesołowski M., Blacha K., Pietruszewski P., Kowalewska A. Wykonanie badania nośności, szorstkości i równości nawierzchni z betonu cementowego wykonanej jako Drogowy Odcinek Lotniskowy, Sprawozdanie nr 24/24/21, ITWL, Warszawa 2021.

ZAKŁADY AUTOMATYKI ®
KOMBUD SA

WWW.KOMBUD.COM.PL

Zakłady Automatyki Kombud SA
ul. Wrocławska 7, 26-600 Radom
+48 48 389 43 01

PDP – POWIADAMIANIE DRÓŻNIKÓW PRZEJAZDOWYCH

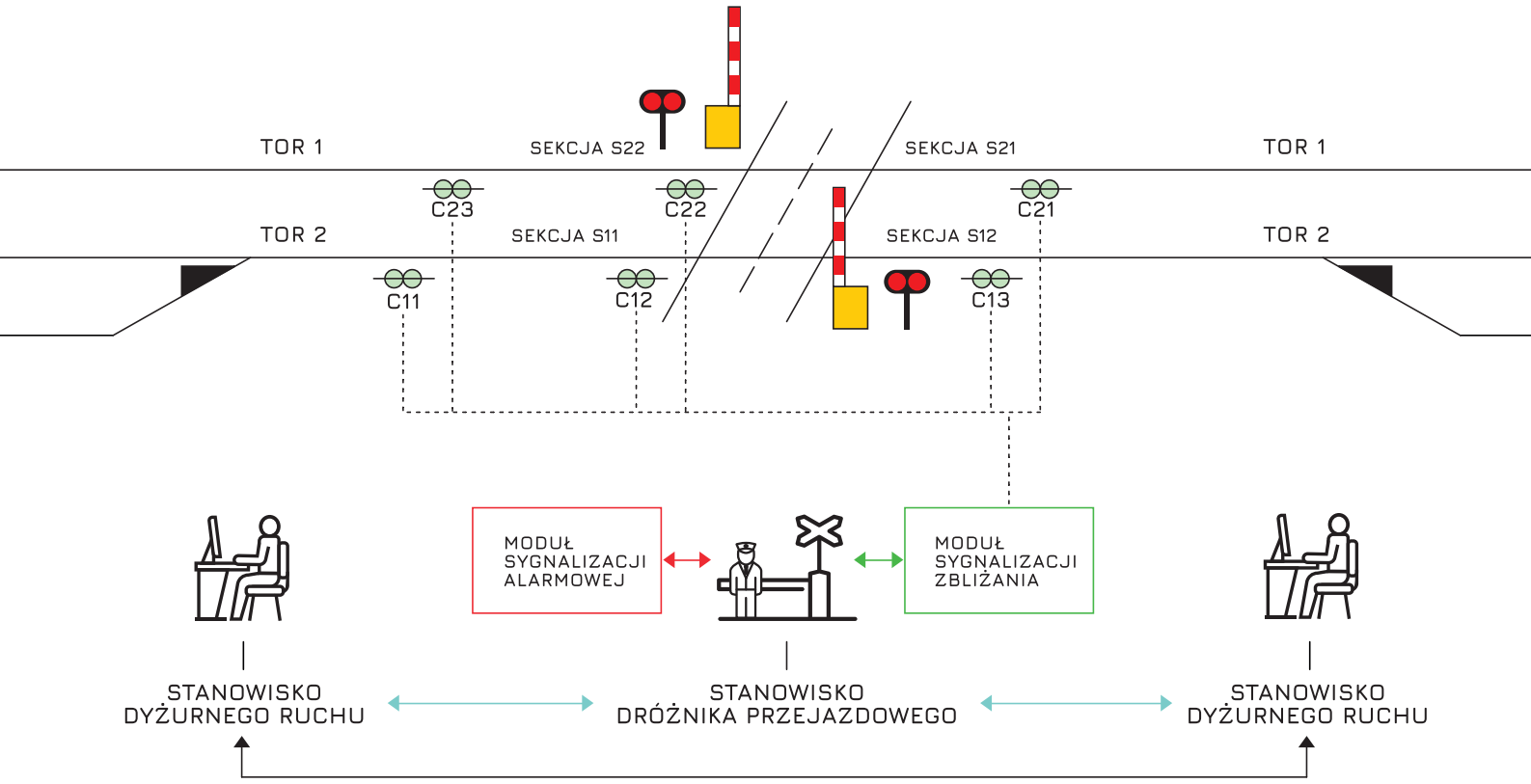
Podnosi poziom bezpieczeństwa i skraca czas zamknięcia przejazdów kolejowych kategorii A.

- dzięki integracji z systemem zdalnego sterowania i kierowania ruchem usprawnia proces prowadzenia ruchu
- pozwala na krótszy czas zamknięcia przejazdu
- zmniejszenie ryzyka wystąpienia błędów ludzkich
- monitoring pracy dróżnika umożliwia zdalną kontrolę jego obecności
- usprawnienie komunikacji z sąsiednimi posterunkami dzięki przesyłaniu informacji o sytuacjach szczególnych

FUNKCJE SYSTEMU PDP:

- dwukanałowa sygnalizacja alarmowa
- mechanizm kontroli obecności
- dwukierunkowa komunikacja
- rejestracja zdarzeń i powiadomień
- administrowanie i kontrola dostępu
- sygnalizacja alarmów i usterek
- samokontrola systemu
- automatyczne informacje dla sąsiednich posterunków

#TRANSFORMUJEMY TRANSPORT



rail-mil.eu

Technologie dostosowane
do potrzeb klienta.

Q7-BL-TR | Eurobalisa przełączalna

Q7 rmRailProtector4.0® | Rozwiązania dla ERTMS | ETCS - L1

Eurobalisa **Q7-BL-TR** produkcji firmy Rail-Mil jest jednym z produktów należących do rodziny **Q7 – rmRailProtector4.0®**, która została zaprojektowana specjalnie z myślą o wymogach oraz funkcjonalności systemów ERTMS i ETCS.

Podstawowe parametry urządzenia:

Eurobalisa o zmniejszonym rozmiarze
Obsługuje uniwersalny interfejs C, zgodny z wymaganiami SUBSET-036, umożliwiający współpracę z koderem LEU dowolnego producenta
Stopień szczelności obudowy IP67
Programowanie odbywa się bezprzewodowo, z wykorzystaniem dedykowanego programatora eurobalis Q7-UPKE
Posiada możliwość zablokowania interfejsu, dzięki czemu staje się niewidoczna dla przejeżdżającego pociągu

Rail-Mil sp. z o.o. jest polską firmą działającą w obszarze elektroniki i automatyki przemysłowej, która skupia się na oferowaniu kompletnych oraz innowacyjnych rozwiązań dla sektora kolejowego i wojskowego. Rozwiązania te oparte są na sprzęcie własnej produkcji, lub od wiodących na rynku zagranicznych partnerów. Naszym głównym celem jest dostarczanie polskich, nowoczesnych i niezawodnych rozwiązań na światowym poziomie dostosowanych do konkretnych potrzeb klienta. W celu zapewnienia najwyższej jakości proponowanych rozwiązań prowadzimy bliską współpracę z najlepszymi jednostkami naukowo-badawczymi w Polsce oraz renomowanymi partnerami zagranicznymi takimi jak m.in.: Ansys Inc., VIAVI Solutions, ERTMS Solutions, RedHat oraz Adlink.

Posiadamy certyfikaty: PN-EN ISO 9001:2015 oraz AQAP 2110:2016

ertms Więcej na temat ETCS i ERTMS: www.ertms.net

made in POLAND

MADE IN EU

rail-mil.eu