

# BIULETYN BEZPIECZEŃSTWA W LOTNICTWIE CYWILNYM

Nr 1(22)/2023



Urząd Lotnictwa Cywilnego

## **W NUMERZE:**

- ✈ materiał na temat cyberbezpieczeństwa w lotnictwie
- ✈ artykuł dotyczący Just Culture w praktyce
- ✈ podsumowanie sprawozdań z wykonywanych zadań lotniczych
- ✈ materiał na temat wykrytych uszkodzeń ścianki Bell 407

## **Publikowane przez:**

Departament Zarządzania Bezpieczeństwem  
w Lotnictwie Cywilnym  
Urząd Lotnictwa Cywilnego  
Ul. Marcina Flisa 2  
02-247 Warszawa  
Tel.: +22 520 75 22

Zapraszamy do zgłaszania  
komentarzy i tematów ważnych  
dla Państwa do poruszenia  
w kolejnych edycjach na adres  
mailowy: **lbb-2@ulc.gov.pl** lub **lbb@ulc.gov.pl**



Szanowni Państwo,

Jest mi niezwykle miło oddać w Państwa ręce kolejny numer Biuletynu Bezpieczeństwa Urzędu Lotnictwa Cywilnego.

W tym wydaniu znajdują Państwo:

- materiał na temat cyberbezpieczeństwa w lotnictwie;
- artykuł dotyczący Just Culture w praktyce;
- podsumowanie sprawozdań z wykonywanych zadań lotniczych;
- materiał na temat wykrytych uszkodzeń ścianki Bell 407.

Wzrost, szczególnie w ostatnim czasie, ataków w cyberprzestrzeni przeciwko polskim i światowym podmiotom gospodarczym oraz stosowanie różnego rodzaju nowych technologii, np. systemów sztucznej inteligencji, wymusza konieczność wprowadzania zmian m.in. w otoczeniu prawnym, również podmiotów prowadzących lotniczą działalność gospodarczą. W artykule Autorzy przedstawili najważniejsze zagadnienia i akty prawne w tej tematyce.

Tematyka Just Culture jest nieodzownym elementem właściwego funkcjonowania kultury bezpieczeństwa a także prawidłowego działania Systemu Zarządzania Bezpieczeństwem w organizacjach, niezależnie od rodzaju wykonywanej działalności. W materiale zaprezentowano praktyczne sposoby, narzędzia a także etapy wdrożenia kultury sprawiedliwego traktowania.

Gromadzenie informacji na temat liczby zrealizowanych zadań lotniczych na poziomie krajowym wynika z obowiązku jaki nakłada art. 135d ustawy Prawo Lotnicze. Od kilku lat sprawozdania przesyłane są w formie elektronicznej z wykorzystaniem wzorów formularzy udostępnianych na stronie internetowej Urzędu Lotnictwa Cywilnego. W związku z tym zaprezentowano podsumowanie danych ze sprawozdań z wykonywanych zadań lotniczych za 2022 rok.

W związku z wykryciem przez organizację zarządzania ciągłą zdatnością do lotu, w trakcie planowej obsługi technicznej śmigłowca Bell 407, rozległego wgniecenia i rozwarstwienia przedniej ściany przedziału bagażowego, przygotowano materiał, w którym Autor opisał dokładnie ww. zdarzenie. Ponadto ze względu na podobieństwo konstrukcji kadłuba, opisywany przypadek może dotyczyć również śmigłowców z rodziny Bell 206.

Zapraszam Państwa do zgłaszania propozycji tematów oraz własnych artykułów związanych z bezpieczeństwem lotniczym - najciekawsze z nich z chęcią opublikujemy na łamach kolejnych wydań Biuletynu. Zachęcam także do dzielenia się swoimi uwagami do opublikowanych materiałów - na Państwa komentarze czekamy pod adresem: [lbb-2@ulc.gov.pl](mailto:lbb-2@ulc.gov.pl) lub [lbb@ulc.gov.pl](mailto:lbb@ulc.gov.pl). Na ten sam adres można również zgłaszać chęć otrzymywania Biuletynu Bezpieczeństwa w Lotnictwie Cywilnym w wersji elektronicznej.

Życzę miłej lektury!

Piotr Samson  
Prezes Urzędu Lotnictwa Cywilnego





## Cyberbezpieczeństwo w lotnictwie cywilnym – aspekt prawny

Wzrost, szczególnie w ostatnim czasie, ataków w cyberprzestrzeni przeciwko polskim i światowym podmiotom gospodarczym oraz niejako równoległe nasilone stosowanie różnego rodzaju nowych technologii, np. systemów sztucznej inteligencji, jak również coraz bardziej zaawansowanych systemów przetwarzania danych, wymusza konieczność wprowadzania zmian m.in. w otoczeniu prawnym również podmiotów prowadzących lotniczą działalność gospodarczą. Wiąże się to z faktem, że technologie są nieodłącznym elementem funkcjonowania i rozwoju lotnictwa cywilnego oraz wpływają na jego bezpieczeństwo i ochronę, jak również na poziom jakości usług świadczonych przez podmioty prowadzące lotniczą działalność gospodarczą. Działania w tym zakresie znajdują odbicie w już przyjętych i formalnie obowiązujących aktach prawnych, jak również w zaawansowanych projektach kolejnych regulacji w zakresie cyberbezpieczeństwa. W tabeli na końcu artykułu zostały przedstawione akty prawne, zdaniem autorów, najważniejsze dla cyberbezpieczeństwa w lotnictwie cywilnym. Należy mieć

na uwadze, że w otoczeniu prawnym podmiotów prowadzących lotniczą działalność gospodarczą w najbliższym czasie pojawią się nowe przepisy, np. Akt o Sztucznej Inteligencji, który będzie regulował m.in. kwestie stosowania systemów sztucznej inteligencji dla zapewnienia bezpieczeństwa i ochrony lotnictwa cywilnego.

Mając na względzie aktualny stan prawny należy wskazać, iż z dniem 31 grudnia 2020 r. weszły w życie przepisy rozporządzenia Wykonawczego Komisji (UE) 2019/1583<sup>1</sup>, które wprowadziły zmiany w przepisach rozporządzenia Wykonawczego (UE) 2015/1998 w zakresie bezpieczeństwa systemów technologii informacyjno – komunikacyjnych i danych krytycznych dla lotnictwa cywilnego. Warto mieć na uwadze, że cytowana powyżej nowelizacja rozp. 2015/1998<sup>2</sup> wpisuje się w szerszą zmianę przepisów dotyczących bezpieczeństwa danych przetwarzanych w formie cyfrowej, którą można obserwować na przestrzeni ostatnich lat. Ich wspólną podstawą powinno być tworzenie spójnego systemu bezpieczeństwa informacji oraz jego pozytywnego wpływu na wzrost

<sup>1</sup>ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/1583 z dnia 25 września 2019 r. zmieniające rozporządzenie wykonawcze (UE) 2015/1998 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego w odniesieniu do środków w zakresie cyberbezpieczeństwa

<sup>2</sup>ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego



poziomu bezpieczeństwa i ochrony w lotnictwie cywilnym, w tym krytycznych informacji przetwarzanych przez podmioty prowadzące lotniczą działalność gospodarczą<sup>3</sup>.

Powyższe obowiązki zostały nałożone na wszystkie podmioty prowadzące lotniczą działalność gospodarczą, które są zobowiązane do posiadania programów ochrony. Oznacza to, że zgodnie z §86 rozporządzeniem Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego, obowiązki te muszą być realizowane przez:

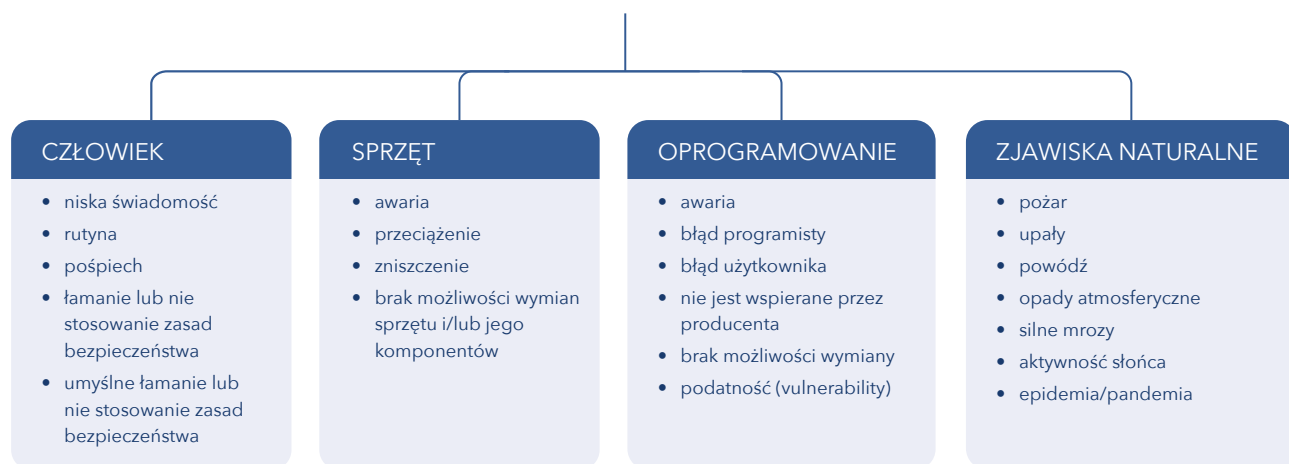
- zarządzających lotniskami,
- przewoźników lotniczych,
- zarejestrowanych agentów,
- znanych nadawców,
- zarejestrowanych dostawców zaopatrzenia pokładowego,
- instytucje zapewniające służby żeglugi powietrznej.

W rozporządzeniu Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 15 marca 2013 r.

w sprawie szczegółowych wymagań dotyczących programów ochrony w lotnictwie cywilnym, które jest uzupełnieniem przepisów rozporządzenia w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego, zostały zawarte rozdziały, które muszą zostać ujęte w programach ochrony podmiotów prowadzących lotniczą działalność gospodarczą. W związku z nowelizacją rozp. 2015/1998, w treści przedmiotowego aktu zostały dodane Rozdziały – Środki ochrony w zakresie cyberbezpieczeństwa.

W związku z tym, podmioty, o których mowa powyżej, zostały zobowiązane do identyfikowania krytycznych lotniczych systemów technologii informacyjno – komunikacyjnych i danych, jak również podjęcia stosownych działań zmierzających do ochrony tych systemów i danych przed cyberatakami. Jednakże należy pamiętać, że nie tylko cyberataki mogą mieć negatywny wpływ na krytyczne lotnicze systemy teleinformatyczne i dane, a w konsekwencji wpłynąć na obniżenie poziomu bezpieczeństwa lotnictwa cywilnego. Przykładowe źródła zagrożeń dla krytycznych lotniczych systemów technologii informacyjno – komunikacyjnych i danych zostały przedstawione na poniższym rysunku.

## ŹRÓDŁA INCYDENTÓW BEZPIECZEŃSTWA



Rysunek nr 1 – Źródła incydentów bezpieczeństwa

<sup>3</sup>Na chwilę obecną systemy cyberbezpieczeństwa podmiotów prowadzących lotniczą działalność gospodarczą funkcjonują w oparciu o dwie, nie do końca spójne, gałęzie prawa nowych technologii – systemy cyberbezpieczeństwa tworzone w oparciu o przepisy Rozporządzenia Wykonawczego Komisji (UE) 2015/1998 oraz systemy cyberbezpieczeństwa tworzone w oparciu o Dyrektywę NIS1. W związku z tym, pojawiła się pilna potrzeba ujednoczenia obu mechanizmów. Wyrazem tego jest przyjęcie przez Komisję Europejską tzw. Rozporządzeń Part-IS. Przepisy te dostępne są na stronach: [https://eur-lex.europa.eu/eli/reg\\_del/2022/1645/oj](https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj) oraz <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R0203>.

Na podstawie aktualnie obowiązującego prawa podmioty prowadzące lotniczą działalność gospodarczą zobowiązane są do określenia krytycznych systemów technologii informacyjno – komunikacyjnych i danych w swoich programach ochrony lub w innym odpowiednim dokumencie, który został wymieniony w programie ochrony<sup>4</sup>. Stworzenie przez podmiot prowadzący lotniczą działalność gospodarczą listy krytycznych systemów technologii informacyjno – komunikacyjnych i danych jest wynikiem procesu, który powinien być oparty o identyfikację wszystkich systemów i danych, które przetwarza organizacja oraz o stosowną ocenę ryzyka, np. *Business Impact Assessment* przeprowadzoną w oparciu o normę ISO 22317.

Następnym krokiem jest przeprowadzenie oceny ryzyka, na podstawie której podmiot prowadzący lotniczą działalność gospodarczą określi i wdroży odpowiednie techniczne i organizacyjne środki bezpieczeństwa mające na celu ochronę krytycznych systemów technologii informacyjno – komunikacyjnych i danych przed cyberzagrożeniami. Stosowane przez podmiot środki bezpieczeństwa muszą, podobnie jak krytyczne systemy teleinformatyczne i dane, zostać określone w programie ochrony lub innym dokumencie wymienionym w programie ochrony. Przykładowe techniczne i organizacyjne środki bezpieczeństwa zostały przedstawione w tabeli nr 1.

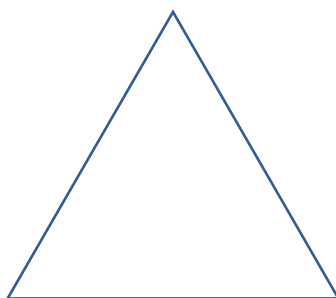
PRZYKŁADOWE TECHNICZNE I ORGANIZACYJNE ŚRODKI BEZPIECZEŃSTWA	
ORGANIZACYJNE ŚRODKI BEZPIECZEŃSTWA	TECHNICZNE ŚRODKI BEZPIECZEŃSTWA
Polityka Bezpieczeństwa Informacji	Program antywirusowy
Polityka czystego biurka	Program antyspamowy
Polityka czystego ekranu	Firewall
Zasady budowania haseł/ Polityka haseł	Zasilanie awaryjne
Polityka kluczy	VPN
Plany postępowania awaryjnego	Szyfrowanie danych
Umowa o zachowaniu poufności	Kopie zapasowe

Tabela nr 1 – Techniczne i organizacyjne środki bezpieczeństwa

<sup>4</sup>Przykładem takiego dokumentu może być Polityka Bezpieczeństwa Informacji czy Rejestr krytycznych lotniczych systemów i danych.

określone dane są **dostępne w dowolnym czasie**  
**i w określony sposób** dla osoby uprawnionej

**DOSTĘPNOŚĆ**  
(ANG. AVAILABILITY)



**POUFNOŚĆ**  
(ANG. CONFIDENTIALITY)

informacja jest **chroniona przed nieuprawnionym dostępem** oraz jej niewłaściwym użyciem

**INTEGRALNOŚĆ**  
(ANG. INTEGRITY)

informacja jest **chroniona przed nieuprawnioną zmianą**

Rysunek nr 2 – Atrybuty Bezpieczeństwa Informacji

Należy również mieć na uwadze, że przepisy prawne w zakresie stosowania środków bezpieczeństwa i ochrony, muszą być neutralne technologicznie. Oznacza to, że przepisy prawne nie mogą narzucać bardzo szczegółowych rozwiązań, które bazują na technologii jednego producenta (m.in. ze względu na ryzyko zarzutu promowania określonych produktów). Stosowane środki bezpieczeństwa i ochrony muszą przede wszystkim chronić poufność, integralność i dostępność stosowanych systemów teleinformatycznych i przetwarzanych danych. Ilustracją pojęć, o których mowa powyżej, jest Rysunek nr 2.

Elementem dopełniającym system cyberbezpieczeństwa, który stworzyły przepisy rozp. 2019/1583, jest pracownik. W zakresie zarządzania personelem, przedmiotowy akt prawny nałożył na podmioty prowadzące lotniczą działalność gospodarczą obowiązek dbania o odpowiedni poziom wiedzy

i umiejętności zatrudnionego personelu. Został również rozszerzony katalog osób, które podlegają standardowemu lub rozszerzonemu sprawdzeniu przeszłości<sup>5</sup>. Istotą tych działań jest zmniejszenie ryzyka ze strony człowieka – najłagodniejszego ogniwa każdego systemu bezpieczeństwa i ochrony. Nowelizacja przepisów rozp. 2015/1998 rozpoczęła proces budowania systemu cyberbezpieczeństwa przez podmioty prowadzące lotniczą działalność gospodarczą. Zobowiązane są one do stworzenia systemu, który ma zapewnić nie naruszalność poufności, integralności i dostępności krytycznych systemów technologii informacyjno – komunikacyjnych i danych, realizując szereg obowiązków wynikających z przepisów prawnych czy kodeksów branżowych.

<sup>5</sup>Zgodnie z pkt. 11.1.2 lit. c) Rozp. 2015/1998, osoby mające uprawnienia administratora lub nieograniczony dostęp bez nadzoru do krytycznych systemów technologii informacyjno – komunikacyjnych i danych muszą przejść rozszerzone lub standardowe sprawdzenie przeszłości z wynikiem pozytywnym. Szczegółowy tryb prowadzenia sprawdzeń przeszłości określają przepisy ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, m.in. art. 189 b ust. 2 pkt. 7 oraz art. 189c ust. 2 pkt. 10.



## AKTY PRAWNE

### PRZYJĘTE PRZEZ KOMISJĘ EUROPEJSKĄ AKT O CYBERBEZPIECZEŃSTWIE

#### Akt o Cyberbezpieczeństwie

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii<sup>6</sup>

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014

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

Tabela nr 3 – Europejskie przepisy w obszarze cyberbezpieczeństwa lotnictwa cywilnego

**Marta Jurkiewicz**  
**Ryszard Tomiak**  
**Departament Ochrony**

<sup>6</sup>Akt ten zostanie zastąpiony Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zmieniająca rozporządzenie (UE) 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148



## Kultura sprawiedliwego traktowania - wdrożenie i praktyczne narzędzia

Celem niniejszego artykułu jest wskazanie praktycznych sposobów wykorzystania narzędzi i opisanie jak powinno wyglądać wdrożenie *Just Culture* w organizacji. W artykule zostaną pominięte kwestie związane z aktami prawnymi, podstawowymi zasadami itp. Znajdziecie je Państwo dokładnie opisane w materiale opublikowanym w Biuletyn Bezpieczeństwa nr 2(16)/2021.

Istotą polityki sprawiedliwego traktowania jest tak naprawdę wyznaczenie i określenie granicy między zachowaniem akceptowalnym a nieakceptowalnym i jasne określenie tego co ma się znajdować po obu jej stronach. Najważniejszym jednak jest kto tę granicę określa i jakie stosuje

zasady, wartości, przepisy etc. Od początku XXI wieku wiele Państw i podmiotów lotniczych przyjęło nowy sposób podejścia do bezpieczeństwa dążąc do osiągnięcia wyższego poziomu dojrzałości w tym zakresie. Wcześniejsze podejście koncentrowało się głównie na indywidualnym poziomie bezpieczeństwa, a nowe kładzie nacisk na zrozumienie złożoności systemu lotniczego oraz różnorodności organizacji, które odgrywają w nim istotną rolę jako elementy budowania wspólnego bezpieczeństwa lotniczego<sup>1</sup>.

W związku z tym, że polityka *Just Culture* ma stać się kręgosłupem, na którym zostanie zbudowany cały system zarządzania bezpieczeństwem musi

<sup>1</sup>ICAO DOC 9859.



ona spełniać szereg warunków. Za jej wdrożenie w organizacji odpowiedzialny jest kierownik odpowiedzialny. Poniżej przedstawiono schemat, według którego wdrożenie polityki sprawiedliwego traktowania powinno się odbywać:

### **1. USTALENIE ASPEKTÓW PRAWNYCH, ZASAD JUST CULTURE I KAR DYSCYPLINARNYCH (powinny być one klarowne).**

Ponadto należy określić kto będzie podejmował decyzje, opracować sposób rozpowszechniania wiedzy na temat zasad i procedur w organizacji. Polityka odnosząca się do *Just Culture* musi być udokumentowana i uwzględniać specyfikę organizacji. W politykach nie powinniśmy używać sformułowań takich jak: osoba „rozsądna” czy tego, że jakaś sytuacja jest „normalna”. Starajmy się, aby zapisy były precyzyjne i unikajmy ogólnych sformułowań. Każda osoba może inaczej zrozumieć daną sytuację lub pojęcie. Ponadto należy wdrożyć sprawiedliwe postępowanie z uwzględnieniem tego kto ocenia sytuację, a także zapewnić niezależność i obiektywizm rozstrzygających<sup>2</sup>.

### **2. OKREŚLENIE FUNKCJI I ZAKRESÓW ODPOWIEDZIALNOŚCI.**

Ważne, żeby właściwie rozróżnić dwa pojęcia, które odnoszą się do odpowiedzialności: *accountability* i *responsibility*. *Accountability* to odpowiedzialność względem kogoś, której nie można scedować na inną osobę. Inaczej jest w przypadku „bycia odpowiedzialnym za coś” (*responsible for*) czyli odpowiedzialności za pewne obowiązki, które możemy przekazać innej osobie. Pamiętajmy, iż polityka odnosząca się do kultury sprawiedliwego traktowania ma zastosowanie do personelu na wszystkich szczeblach organizacyjnych.



### **3. USTANOWIENIE JAK MAJĄ WYGLĄDAĆ PROCEDURY RAPORTOWANIA (struktura, przepływ informacji i zasady poufności).**

Anonimowość oznacza, że tożsamość osoby zgłaszającej jest nikomu nieznaną. Z kolei poufność oznacza, że osoba zgłaszająca wypełnia rubryki z imieniem, nazwiskiem i przynależnością do danej jednostki tym samym stając się znanym tym, którzy takie zgłoszenie otrzymują. Początkiem i bardzo ważnym krokiem w zakresie zgłoszeń dobrowolnych było podpisanie w 1976 r. porozumienia pomiędzy NASA (Narodową Agencją Aeronautyki i Przestrzeni Kosmicznej) a FAA (Federalną Administracją Lotnictwa Stanów Zjednoczonych) o ustanowieniu systemu raportowania, w którym pracownicy mogą

<sup>2</sup>Zgodnie z art.16 ust. 11 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 376/2014 z dnia 3 kwietnia 2014 r. „Wewnętrzne przepisy dotyczące kultury sprawiedliwego traktowania organizacja przyjmuje po konsultacji z przedstawicielstwem pracowników”.



dobrowolnie i bez ponoszenia konsekwencji dokonywać zgłoszeń zdarzeń<sup>3</sup>. Systemy raportowania powinny być połączone z *Just Culture*. Koniecznym jest stosowanie zasady, że zbierane dane i informacje zawarte w zgłoszeniach mogą być wykorzystywane jedynie w celu utrzymania lub poprawy poziomu bezpieczeństwa w lotnictwie.

Pamiętajmy, iż trudno określić, który system i jaka metoda raportowania będą najlepsze dla danej organizacji i należy podejść do tego elastycznie (łatwiej zachować poufność i anonimowość w dużej organizacji).

#### **4. OPRACOWANIE FORMULARZA RAPORTU.**

Formularz raportu ma zachęcać do raportowania, a pytania powinny być klarowne i bardzo precyzyjne. Ponadto należy ustalić:

- jakie informacje chcemy zbierać,
- co chcemy robić z tymi informacjami,
- w jakiej formie informacje mają być przekazywane,
- jakie zasoby są potrzebne do „obróbki” informacji.

Należy także określić czy i w jaki sposób formularz raportu będzie zintegrowany z obecnym systemem raportowania zespołu odpowiedzialnego za system i ustanowienie tzw. „*focal point*” / „*goal keeper*” czyli osoby / osób, które będą miały dostęp do pełnych danych zgłaszającego. Ważnym elementem jest opracowanie szablonu informacji zwrotnej dla raportujących. Nawet niedoświadczeni pracownicy muszą być świadomi, że raportowanie incydentów jest ważne dla budowania właściwej kultury bezpieczeństwa, a feedback jest ważnym elementem zachęcania do partycypowania w systemie.

#### **5. USTALENIE PLANU SZKOLENIA PERSONELU I OPRACOWANIE ZAKRESU SZKOLEŃ DLA WSZYSTKICH PRACOWNIKÓW.**

Szkoleniem obowiązkowym jest zawsze przeszkolenie z czynnika ludzkiego i podstaw SMS. To czy tematyka szkolenia ma być rozszerzona dla danego pracownika zależy od funkcji tej osoby w systemie. Można też omówić jego zakres z osobą, której szkolenie ma dotyczyć. Ponadto przy promocji bezpieczeństwa należałoby się zastanowić / przetestować jaki rodzaj komunikacji będzie odpowiedni dla naszej organizacji oraz danej grupy pracowników / obszaru działalności<sup>4</sup>.

#### **6. USTANOWIONY I UZGODNIONY SPOSÓB POSTĘPOWANIA ODNOŚNIE PERSONELU, KIEROWNICTWA, ZWIĄZKÓW ZAWODOWYCH I ORGANIZACJI PRACOWNICZYCH.**

Często to czy pracownicy uznają reakcję kierownictwa za sprawiedliwą, zależy nie tyle od samej reakcji, ale też od relacji panujących między kierownictwem a pracownikami.

#### **7. ROZWIJANIE I KONSEKWENTNE PODTRZYMANIE USTALONYCH ZASAD.**

<sup>3</sup>Strona internetowa FAA: <https://www.faa.gov/newsroom/aviation-voluntary-reporting-programs-1>. [Dostęp: 3.03.2023].

<sup>4</sup>Dokładniej ten temat jest opisany w ICAO DOC 9859 w rozdziale 9, punkt 9.6 i przykładowym Podręczniku SMS- Rozdział 4.2. Zachęcamy także do zapoznania się z prezentacją dostępną na stronie internetowej ULC dotyczącej promocji bezpieczeństwa.

SPOSÓB POSTĘPOWANIA	OBJAŚNIENIE	KONSEKWENCJE POSTĘPOWANIA
Działanie z premedytacją	Działanie wykonywane z intencją spowodowania wypadku / zranienia ludzi.	Cofnięcie upoważnienia / (Natychmiastowe zwolnienie/ Postępowanie karne)
Działanie ze świadomością konsekwencji	Działanie, podczas którego popełniono błąd – osoba jest świadoma tego błędu. Osoba jest również świadoma, że jej działanie może prowadzić do wypadku (jest to prawdopodobne).	Działania muszą być podjęte. (Cofnięcie upoważnienia/ możliwe zwolnienie lub zawieszenie)
Działanie pod wpływem narkotyków lub alkoholu	Każde działanie, które prowadzi do wypadku, podczas gdy osoba jest pod wpływem alkoholu lub narkotyków.	Polityka musi jasno określać, że jest to zachowanie niedopuszczalne. Muszą być podjęte działania dyscyplinarne.
Działanie lekkomyślne	Działanie wykonywane ze świadomym zlekceważeniem ryzyka, że może ono poważnie i w nieusprawiedliwiony sposób zwiększyć prawdopodobieństwo wystąpienia wypadku.	Muszą być podjęte działania dyscyplinarne. (Zawieszenie upoważnienia/ degradacja zawodowa lub ostateczne upomnienie)
Wielokrotne zaniedbania (niedbalstwo)	Kumulacja działań o charakterze zaniedbania lub akt niedbalstwa, który kreuje więcej możliwości wystąpienia wypadku.	Muszą być podjęte działania dyscyplinarne. (Upoważnienie może być zawieszona/ upomnienie, możliwa degradacja)
Niedbalstwo	Sytuacja, kiedy osoba powinna była zdawać sobie sprawę, że jej działania mogą poważnie i w nieusprawiedliwiony sposób zwiększyć ryzyko wystąpienia wypadku.	Okoliczności mogą, ale nie muszą wymagać podjęcia działań dyscyplinarnych. (Pouczenie / Upomnienie)
Odmowa udziału w dochodzeniu (badanie zdarzeń/ błędów).	Kiedy odmowa udziału w dochodzeniu wynika z powodów, które mogłyby wskazać, że czyn był w kategorii wyższego poziomu winy.	Jeśli jest dowiedzione, że miała miejsce próba zatuszowania faktów, muszą być podjęte działania dyscyplinarne. (Formalne upomnienie)
Błąd	Kiedy doszło do aktywnego błędu, który został popełniony na skutek nieprzestrzegania procedur przez jednostkę. Również w sytuacji, kiedy błędnie napisana procedura doprowadziła do popełnienia błędu	(Pouczenie wszystkich - jeśli występują podobne błędy) Jeśli procedura była nieprawidłowa – żadne działania dyscyplinarne nie będą podejmowane. Procedura musi być poprawiona.
Pomyłka (potyczka, niedopatrznie)	Błąd w rozpoznaniu (świadomość sytuacyjna), związany z pamięcią lub uwagą – na przykład na skutek zmęczenia.	Działania dyscyplinarne nie będą podejmowane.
Brak uchybienia	Zauważenie i określenie uśpionego błędu (w systemie)	Pochwała/ nagroda dla raportującego

Zgodnie z powyższym schematem widzimy w jaki sposób powinno odbywać się ocenianie pewnych postaw.

Zachowania znajdujące się na niebieskim polu są zachowaniami o najwyższym stopniu zawinienia, z kolei te na szarym tle prezentują najniższy poziom zawinienia. Należy pamiętać, że ocena ludzkich zachowań jest dość delikatną materią i do każdej sytuacji trzeba podchodzić indywidualnie. To czy dana osoba powinna być pociągnięta do odpowiedzialności będzie zależęć przede wszystkim od stopnia jej wykszolenia, kwalifikacji i świadomości danej sytuacji podczas wystąpienia zdarzenia. Tu musimy brać pod uwagę występowanie tzw. efektu pewności wstecznej – gdy oceniamy sytuację nie pod kątem wiedzy, którą ktoś miał w danym momencie, a posiadając pełny obraz sytuacji i wszystkie potrzebne informacje. Ponadto, jak przedstawiono wyżej, przy ocenie zachowań bardzo jasno musimy określić zasady, według których dokonujemy tejże oceny, a także jakie zachowania będziemy karać, a jakie nagradzać: Np. wiedzę na temat obecnego systemu

– jeśli jest ona wysoka – nagradzamy. Musimy pamiętać o wyróżnianiu dyscypliny, dokładności, spójności i chęci do nauki szczególnie tych osób, które dobrze rozumieją system i chętnie dzielą się swoim doświadczeniem. Pamiętajmy, iż stwierdzenie, że zachowanie jest lekkomyślne, błędne bądź niedbałe jest naszą oceną działań innej osoby, a nie opisem istoty jej zachowania. Nie możemy traktować ww. zachowań jako stałych w postępowaniach ludzi. Przy ocenie danej sytuacji na pewno należy się zastanowić czy zdarzyła się ona po raz pierwszy. Jeśli dana osoba nie ma doświadczenia, to nie powinniśmy jej za to karać. Co więcej zastanówmy się czy inne osoby / współpracownicy zwracali już wcześniej na to uwagę.

Należy promować takie postawy, które pozwolą uczyć się na błędach. W sytuacji gdy np. zastosowano niewłaściwą procedurę (działanie świadome, ale przyjęto błędne założenia) możliwym jest, że były one dla kogoś niezrozumiałe. Same procedury powinny być wykorzystywane jako materiał, który stosujemy dopóki nie jesteśmy ekspertami w danej dziedzinie.





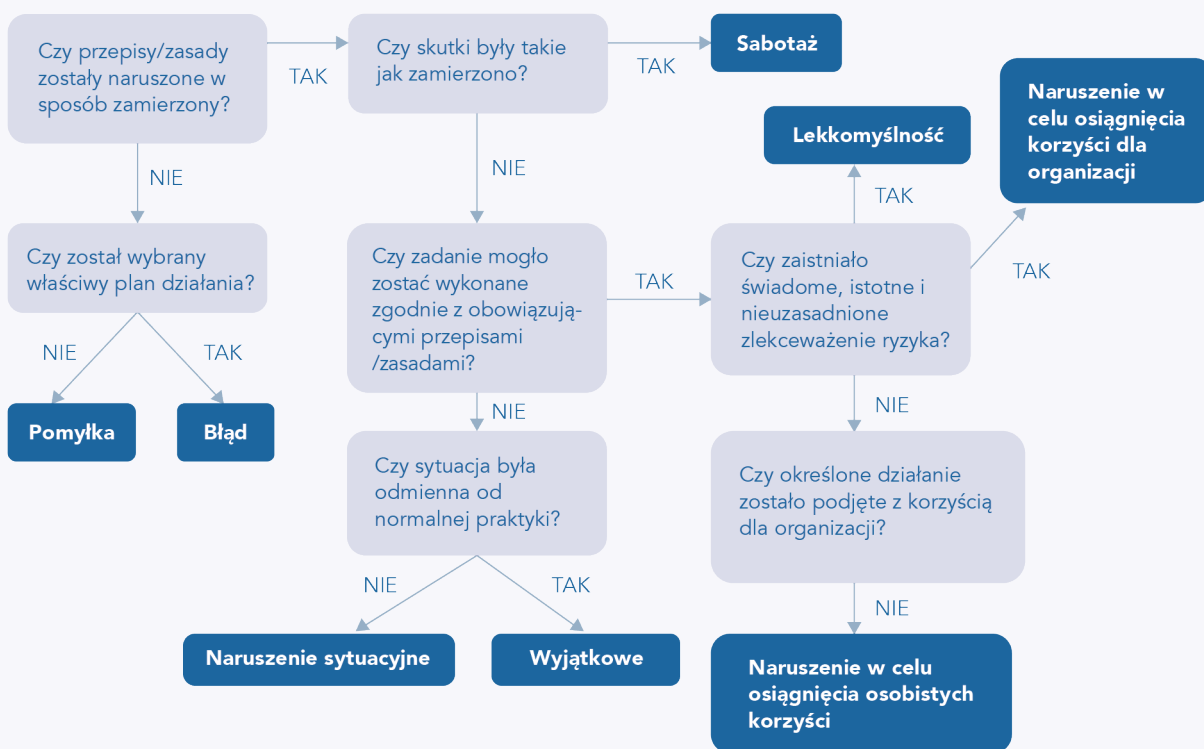
Jeżeli chcemy je zmieniać / uzupełniać to ważne, żeby mieć pewność, że dokonujemy ulepszenia systemu, a nie jego przypadkowego pogorszenia. Musimy być czujni i nie przepuścić takiej szansy żeby nie stało się tak, że pewne odchylenia i łamanie procedur staną się normą i złym nawykiem w budowaniu kultury bezpieczeństwa.

u operatora lotniczego. Zadanie to będzie realizowane na podstawie narzędzia SM-ICG „Industry Safety Culture Evaluation Tool and Guidance”. Właściwie budowana kultura bezpieczeństwa to niekończący się proces. Odpowiednio wdrażana, propagowana może przyczynić się nie tylko do poprawy stanu bezpieczeństwa, ale także wyge-

Kolejnym narzędziem, które może nam pomóc w ocenie zachowań i ustaleniu stopnia współodpowiedzialności jest Narzędzie FAiR (Flowchart Analysis of Investigation Results). Pozwala ono nieco uporządkować „proces” oceny, tak by nie zapomnieć o żadnych istotnych elementach.

## Narzędzie FAiR

(Flowchart Analysis of Investigation Results)



Nie możemy zapominać, iż kultura sprawiedliwego traktowania jest częścią kultury bezpieczeństwa. W EPAS (European Plan for Aviation Safety) 2023-2025 EASA wprowadziła zadanie dotyczące monitorowania kultury bezpieczeństwa

nerowania większych zysków finansowych. Do oceny czy w naszej organizacji istnieje i rozwijana jest kultura bezpieczeństwa może nam posłużyć poniższy model:

## SAFETY CULTURE

Opis postaw/ zachowań i wskaźniki występowania

OPIS	WSKAŹNIKI
Zaangażowanie	<ul style="list-style-type: none"> <li>– traktowanie bezpieczeństwa priorytetowo</li> <li>– stosowanie procedur bezpieczeństwa</li> <li>– zaangażowanie personelu i odpowiedzialność za bezpieczeństwo</li> </ul>
Zachowanie	<ul style="list-style-type: none"> <li>– zachowanie personelu z poszanowaniem zasad bezpieczeństwa</li> <li>– zadowolenie z pracy</li> </ul>
Świadomość	<ul style="list-style-type: none"> <li>– świadomość zachowań, które mogą powodować ryzyko</li> <li>– troska o bezpieczeństwo</li> </ul>
Adaptacja/Dostosowanie	<ul style="list-style-type: none"> <li>– postawa proaktywna w celu uniknięcia negatywnych sytuacji i zdarzeń</li> <li>– wkład pracowników</li> </ul>
Informowanie	<ul style="list-style-type: none"> <li>– dostęp do informacji</li> <li>– szkolenia</li> <li>– działający system raportowania zdarzeń dotyczących problemów/ kwestii bezpieczeństwa</li> <li>– chęć korzystania z systemu raportowania</li> <li>– określenie konsekwencji raportowania zdarzeń</li> </ul>
Słuszność/Zasadność	<ul style="list-style-type: none"> <li>– ocena zachowań związanych / dotyczących bezpieczeństwa</li> <li>– punkt widzenia / odniesienia oceny dotyczącej negatywnych zachowań</li> <li>– przekazywanie odpowiedzialności</li> </ul>

Wewnętrzne przepisy dotyczące kultury sprawiedliwego traktowania powinny wskazywać na wyjątki od zwolnienia od „taryfy ulgowej”. Dobrą praktyką jest określenie konkretnych przykładów takich zachowań, tak by były zrozumiałe dla personelu. Musimy pamiętać, iż takie same przyczyny mają incydenty jak i wypadki. Nie jesteśmy w stanie przewidzieć każdej sytuacji, która może się zmaterializować. Incydent w organizacji nie może być postrzegany jako porażka lub sytuacja kryzysowa tylko pewnego rodzaju szansa na naukę. Ponadto dokonując oceny zachowań należy pamiętać, że z założenia ludzie przychodzą do pracy, aby dobrze wykonywać swoje obowiązki.

Nie można zapominać także, że poziom bezpieczeństwa generują osoby, które tworzą system

i używają go. Otoczenie i środowisko w organizacji powinno umożliwiać podejmowanie działań w przypadku gdy są one niezbędne dla utrzymania lub poprawy poziomu bezpieczeństwa lotniczego, uwzględniając zasady kultury bezpieczeństwa. Pamiętajmy, iż bezpiecznie nie oznacza bez ryzyka, a bez odpowiednio wdrożonej kultury sprawiedliwego traktowania nie do końca wiemy co się dzieje w naszej organizacji i czy rzeczywiście mamy kontrolę nad zagrożeniami.

**Klaudia Cyran**  
**Departament Zarządzania Bezpieczeństwem**  
**w Lotnictwie Cywilnym**

# BUSINESS REPORT

92%

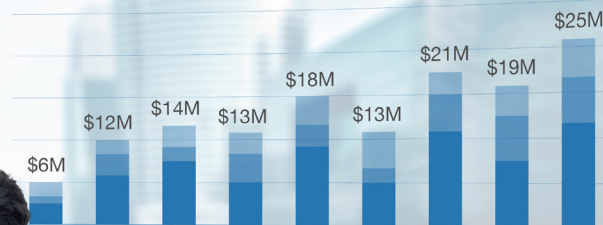


95%



Evolution	Metric	Actual vs Target	Actual	Target
	Revenue		\$3.4M	82.0%
	Profit		\$1.2M	108.7%
	Avg. Order Size		\$850.3	71.0%
	On Time Delivery		96.0%	96.0%
	New Customers		15432	145.0%
	Cust. Satisfaction		98.3%	105.0%

## Performance



## Sales per countries



## Top 8 products



## Podsumowanie zadań lotniczych wykonywanych w 2022 roku

Gromadzenie informacji na temat liczby zrealizowanych zadań lotniczych na poziomie krajowym za miniony rok wynika z obowiązku jaki nakłada art. 135d ustawy Prawo Lotnicze. Sprawozdania są formą deklaracji ze strony użytkownika, zawierają one dane dotyczące liczby operacji i nalotu na poszczególnych statkach powietrznych i rodzaju wykonywanych operacji. Od kilku lat sprawozdania przesyłane są w formie elektronicznej z wykorzystaniem wzorów formularzy udostępnianych na stronie internetowej Urzędu Lotnictwa Cywilnego<sup>1</sup>.

**Wszyscy użytkownicy statków powietrznych zgodnie z art. 135d. ustawy z dnia 3 lipca 2002 r. Prawo Lotnicze, które podlegają wpisowi do rejestru statków, składają Prezesowi Urzędu Lotnictwa Cywilnego w terminie do 31 stycznia każdego roku sprawozdania, za miniony rok z wykonywania operacji lotniczych.**

<sup>1</sup>Link: <https://ulc.gov.pl/pl/zarzadzanie-bezpieczenstwem/sprawozdania-z-wykonywania-zadan-lotniczych/6053-formularze-sprawozdan-z-wykonywania-zadan-lotniczych-za-2022-rok>



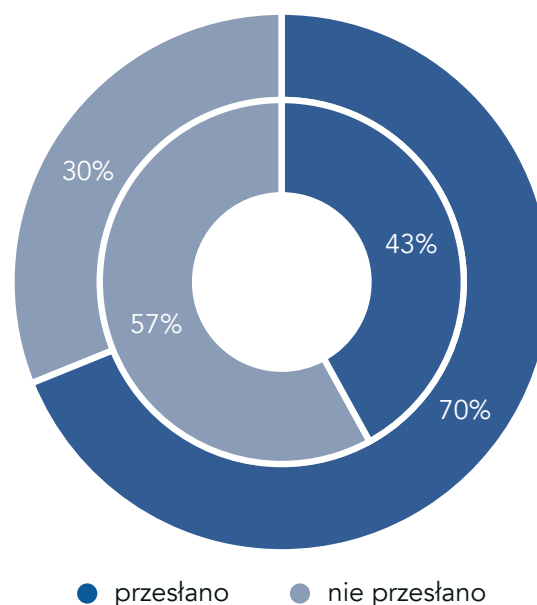
Kategoria statku powietrznego	2021		2022	
	Liczba SP w rejestrze 2021 r.	Liczba SP zgłoszonych w sprawozdaniach 2021 r.	Liczba SP w rejestrze 2022 r.	Liczba SP zgłoszonych w sprawozdaniach 2022 r.
<b>Samoloty</b>	1504	812	1533	821
<b>Śmigłowce</b>	275	123	285	118
<b>Szybowce</b>	1057	429	1077	395
<b>Motoszybowce</b>	44	11	47	14
<b>Balony</b>	265	29	287	55
<b>Razem</b>	<b>3145</b>	<b>1404</b>	<b>3229</b>	<b>1403</b>

Tabela 1. Liczba statków powietrznych w krajowym rejestrze w latach 2021 i 2022.

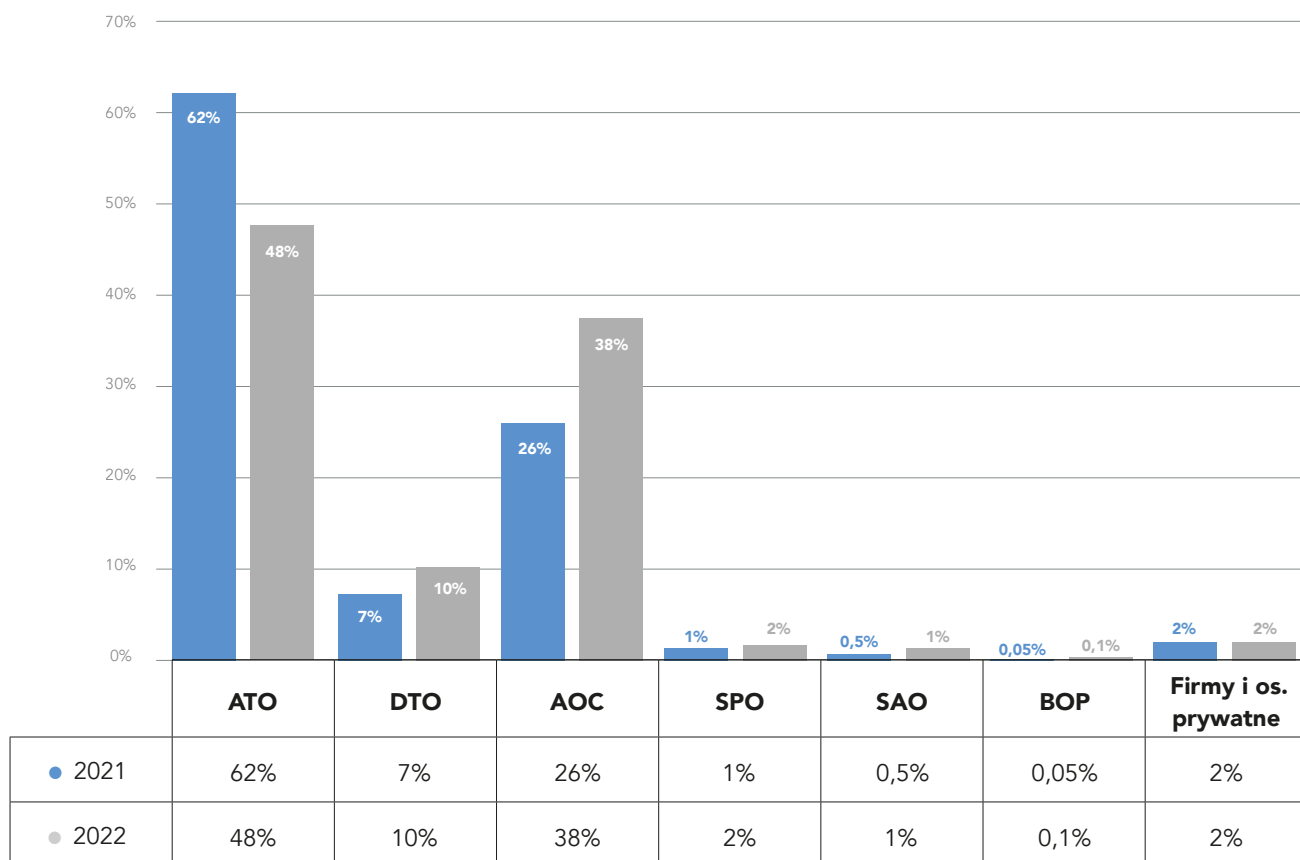
Powyższe podsumowanie zostało przygotowane w oparciu o wykaz polskich statków powietrznych w rejestrze cywilnych statków powietrznych ULC oraz wykaz certyfikowanych podmiotów lotniczych. Jednocześnie zgromadzone dane zostały zagregowane do całkowitej liczby operacji wykonywanych dla poszczególnych kategorii statków powietrznych zarówno w ramach zarobkowej działalności lotniczej (przewóz osób lub inne usługi lotnicze), jak i w ramach szkolenia w ośrodkach szkolenia lotniczego, oraz przez firmy i organizacje niekomercyjne i osoby prywatne. W powyższej Tabeli 1 można zapoznać się z ogólną statystyką dotyczącą liczby statków powietrznych w krajowym rejestrze prowadzonym przez Urząd Lotnictwa Cywilnego oraz ujętych w sprawozdaniach w 2022 roku i porównanie tych danych do roku 2021.

Pierwsza analiza (Wykres 1) przedstawia liczbę sprawozdań przesłanych przez podmioty lotnicze w stosunku do aktualnego wykazu organizacji zarejestrowanych w Urzędzie oraz udział procentowy

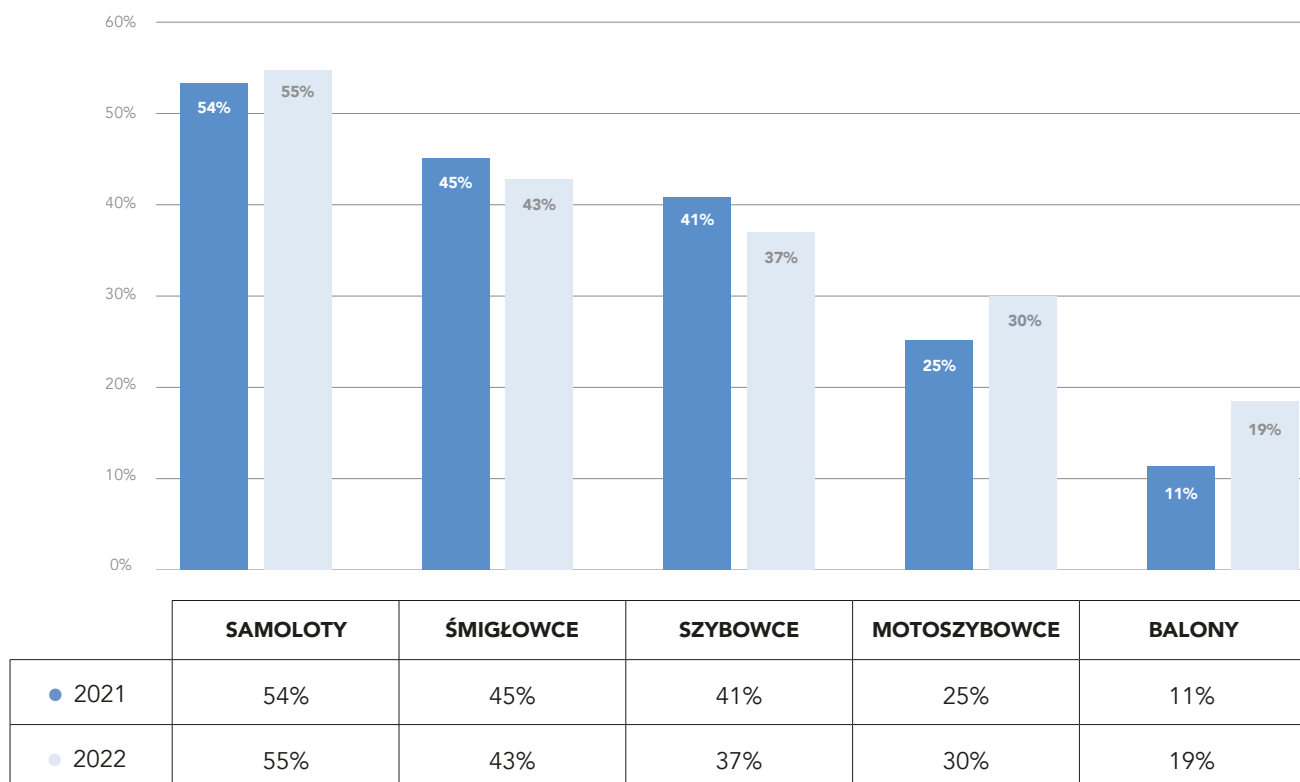
1. Pierścień zewnętrzny - liczba podmiotów lotniczych
2. Pierścień wewnętrzny - liczba statków powietrznych



Wykres 1. Liczba przesłanych sprawozdań przez certyfikowane podmioty lotnicze (pierścień zewnętrzny) oraz (pierścień wewnętrzny) za 2022 rok.



Wykres 2. Udział procentowy liczby operacji lotniczych wykonywanych przez certyfikowane podmioty lotnicze oraz firmy niekomercyjne i osoby prywatne – porównanie 2022 i 2021.



Wykres 3. Udział procentowy liczby statków powietrznych ujętych w sprawozdaniach w stosunku do liczby SP w rejestrze ULC – porównanie 2022 i 2021.

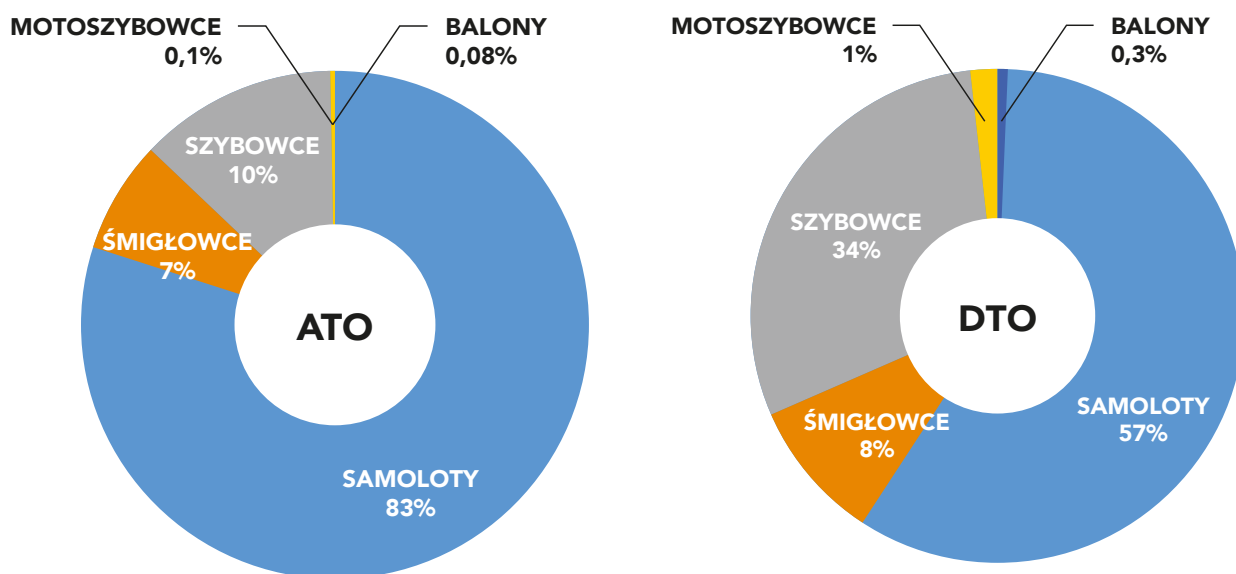
statków powietrznych ujętych w sprawozdaniach w stosunku do całkowitej liczby statków powietrznych w rejestrze ULC. W wyniku licznych powiadomień o składaniu sprawozdań z wykonywanych zadań, liczba sprawozdań przesyłanych przez organizacje lotnicze do Prezesa ULC kształtuje się na poziomie 70%. Tymczasem dane dotyczące nalotów statków powietrznych uzyskano jedynie na poziomie 43% w stosunku do aktualnego rejestru ULC.

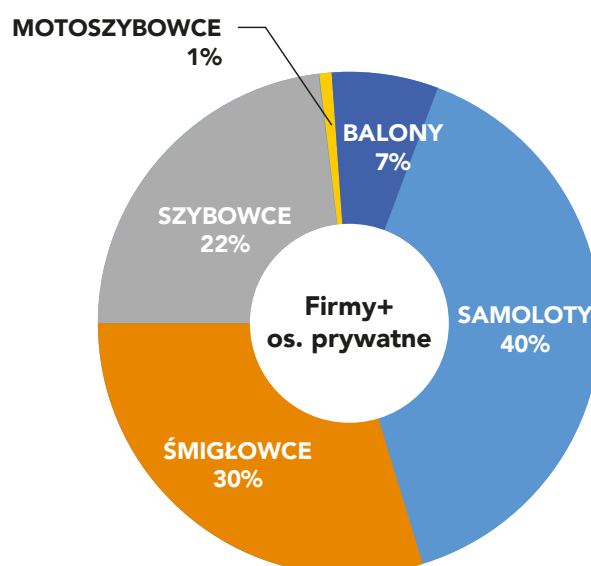
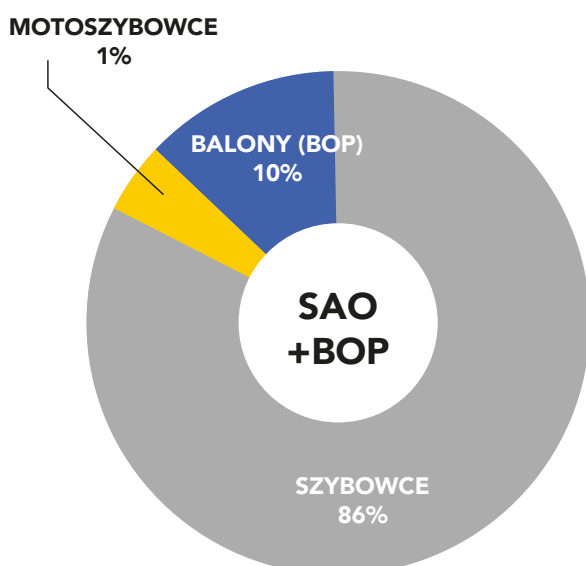
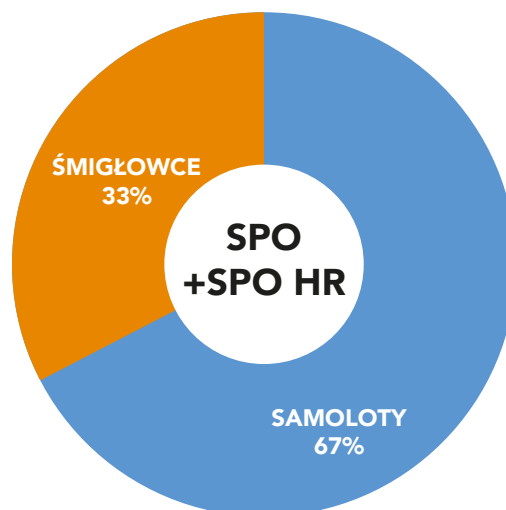
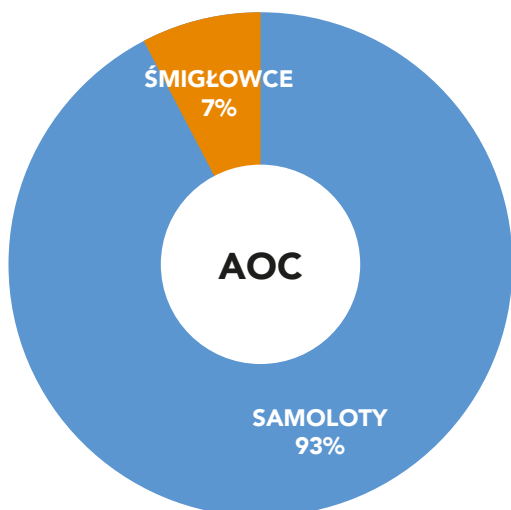
Kolejne porównanie dotyczy liczby operacji lotniczych wykonywanych przez certyfikowane podmioty lotnicze w okresie dwóch ostatnich lat (Wykres 2). Zarówno w 2021 jak i 2022 roku najwięcej operacji lotniczych odbyło się w certyfikowanych ośrodkach szkolenia lotniczego ATO oraz w ruchu pasażerskim w ramach certyfikatu AOC. Pomimo, że nie wszystkie podmioty lotnicze przesyłały sprawozdania to można zaobserwować wyraźny wzrost operacji lotniczych o 12% w zakresie certyfikatu AOC oraz mniejszy udział operacji lotniczych o 14% w certyfikowanych ośrodkach szkolenia ATO w stosunku do 2021 roku.

Wykres 3 przedstawia udział procentowy danych dla poszczególnych kategorii statków powietrznych w stosunku do liczby statków powietrznych będących w rejestrze ULC. Wyłącznie dla samolotów ponad połowa (55%) została ujęta w sprawozdaniach za 2022 r. W przypadku innych kategorii statków powietrznych: dane nalotowe dla śmigłowców przesłano na poziomie 43%, szybowców na poziomie 37%, motoszybowców na poziomie 30% oraz dla balonów zaledwie na poziomie 19%.

Poniższe zestawienia na wykresach kołowych przedstawiają udział procentowy liczby wykonanych operacji lotniczych na poszczególnych kategoriach przez podmioty lotnicze w ramach posiadanych certyfikatów w 2022 roku. Warto zwrócić uwagę i porównać działalność szkoleniową w certyfikowanych podmiotach ATO oraz zadeklarowanych ośrodkach DTO. Pomimo, że w obu przypadkach najwięcej operacji lotniczych dotyczy szkoleń do uzyskania licencji na samolot lub na szybowiec, to w ośrodkach szkolenia DTO można zaobserwować wielokrotnie większy udział zadań lotniczych w stosunku do ośrodków szkolących ATO.

Zestawienie wykresów przedstawiających udział realizacji zadań lotniczych na określonym typie statków powietrznych w poszczególnych obszarach działalności lotniczej.





Realizacja procesu przesyłania sprawozdań z zadań lotniczych za miniony rok przez certyfikowane podmioty lotnicze okazała się być na nieco niższym poziomie w odniesieniu do roku 2021. Wśród najważniejszych porównań należy wymienić poziom sprawozdawczości (Wykres 1) oraz udział zrealizowanych operacji lotniczych na określonym typie statku powietrznego w poszczególnych obszarach działalności lotniczej (zestawienie wykresów). Należy mieć na uwadze, że przedstawione dane ujęte w powyższych statystykach dotyczą jedynie części statków powietrznych (Tabela 1), dlatego

przedstawione statystyki mogą się różnić od faktycznej ilości eksploatowanych statków powietrznych oraz faktycznego ruchu lotniczego i rodzaju wykonywania zadań lotniczych (szkolenie, usługi i przewóz lotniczy oraz loty rekreacyjne i prywatne).

**Łukasz Kornas**  
**Departament Zarządzania Bezpieczeństwem**  
**w Lotnictwie Cywilnym**

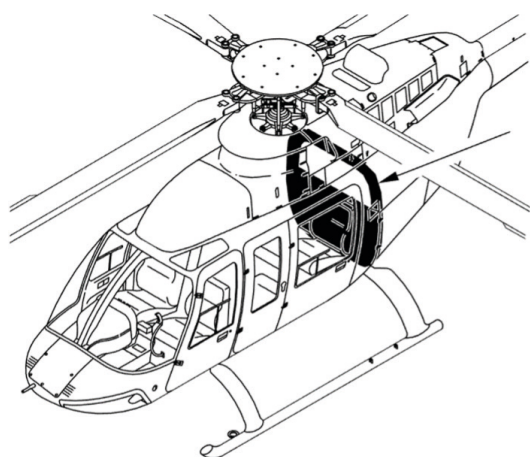




## Kosztowny bagażnik śmigłowca Bell 407

Lekkie śmigłowce wykorzystywane do celów prywatnych często traktowane są jak samochód - narzędzie służące do codziennego przemieszczania się, któremu w pewnych kwestiach nie poświęca się wiele uwagi. Jedną z takich kwestii jest przewożenie bagażu - bo kto z nas zawsze zwraca uwagę na to czy walizka którą wkładamy do bagażnika auta nie uderza wtedy w jedną ze ścian? Bagażnik jest z zasady kojarzony z przestrzenią typowo użytkową i zwykle nikt nie

przejmuje się z nadto tym w jaki sposób wkłada do niego bagaż. Otwieramy klapę, wrzucamy walizkę, zamykamy i jedziemy. O ile zwykle piloci wiedzą jak prawidłowo załadować i zabezpieczyć bagaż, niejednokrotnie jest on wkładany do bagażnika przez pasażerów, którzy traktują go w ten sam sposób co bagażnik auta – i może być to przyczyną wielu problemów.



Rysunek 1 Lokalizacja panelu P/N 407-030-512-101

Jedna z zatwierdzonych organizacji zarządzania ciągłą zdadnością do lotu opublikowała biuletyn bezpieczeństwa po tym, jak w trakcie planowej obsługi technicznej śmigłowca Bell 407 odnaleziono rozległe wgniecenia i rozwarstwienia przedniej ściany przedziału bagażowego (panel P/N 407-030-512-101A – Rysunek 1, Zdjęcie 1). Uszkodzenia roziane były niemal po całej powierzchni ściany i prawdopodobnie powstały wskutek nieprawidłowego załadunku bagażu lub przemieszczania się go w trakcie lotu. **Ze względu na podobieństwo konstrukcji kadłuba, opisany przypadek może dotyczyć również śmigłowców z rodziny Bell 206.**

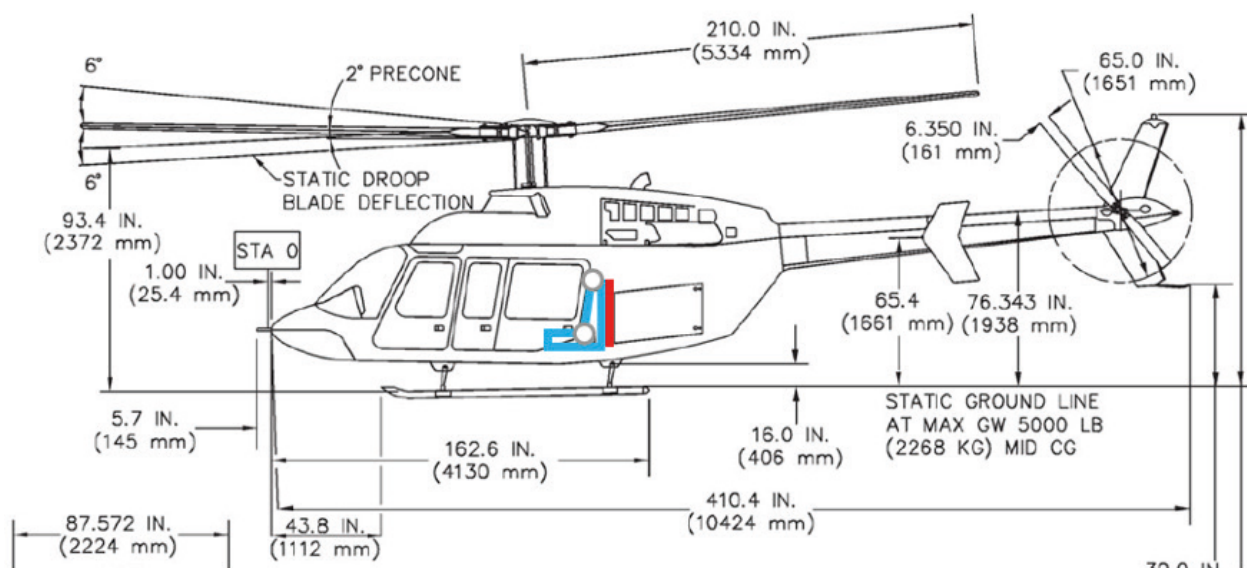


Zdjęcie 1 Wyraźnie widoczne liczne wgniecenia na obszarze całej ściany.

Panel P/N 407-030-512-101A pozornie wydaje się być jedynie ścianą bagażnika – i w istocie jest ścianą bagażnika, ale jednocześnie stanowi element podstawowej struktury kadłuba śmigłowca. Panel jest elementem wręgi kadłuba P/N 407-030-505-185, która przyjmuje obciążenia od podwozia i wspiera tylną część belki dachowej, która wspiera przekładnię główną i inne podzespoły zamontowane na górnym pokładzie śmigłowca.

W dodatku, oddziela bagażnik od tylnej komory zbiornika paliwa, zlokalizowanej od strony kabiny pasażerskiej.

Panel jest konstrukcją kompozytową, zbudowaną z wypełniacza ulowego i aluminiowego poszycia. Jak w przypadku wszystkich kompozytów, zachowuje on swoje właściwości pod warunkiem utrzymania integralności konstrukcji. Wgniecenia i rozwarstwienia panelu mogą wpłynąć na jego wytrzymałość i w konsekwencji na wytrzymałość całej wręgi kadłuba. W przypadku wystąpienia twardego lądowania wręga może nie przenosić odpowiednio obciążeń, co potencjalnie doprowadzić może do uszkodzenia zbiornika paliwa i stworzenia zagrożenia pożarowego. Przy silnym uderzeniu o ziemię nie można również wykluczyć ryzyka zapadnięcia przekładni głównej do kabiny pasażerskiej, znajdującej się bezpośrednio poniżej, jako że wręga wspiera tylną część belki dachowej. Oprócz zagrożenia dla bezpieczeństwa załogi i pasażerów, niniejsza sytuacja wiąże się z poważnymi kosztami naprawy. W przypadku niewielkich uszkodzeń ścianę można naprawić – jednakże w omawianym przypadku niezbędna była jej wymiana ze względu na zbyt duży obszar uszkodzeń. Do



Rysunek 3 Lokalizacja panelu P/N 407-030-512-101 (czerwony) i głównej komory zbiornika paliwa (niebieski)

wymiany ściany wymagane jest wykorzystanie zatwierdzonego przez firmę Bell uchwytu do kadłuba - dostępne są jedynie w kilku organizacjach obsługowych w Ameryce Północnej. Zatem koszt demontażu głównych podzespołów śmigłowca, wymiany ściany i malowania, w przypadku europejskiego operatora, zostaje dodatkowo zwiększony o koszt transportu śmigłowca do Kanady lub Stanów Zjednoczonych – całkowity koszt takiej operacji sięgać może kwoty kilkuset tysięcy dolarów.

Aby zapobiec wymienionym powyżej zagrożeniom ważna jest odpowiednia profilaktyka. Na rynku jest dostępnych kilka certyfikowanych ochroniaczy montowanych na ścianę bagażnika, które mogą zapobiec uszkodzeniom i uniknąć wysokich kosztów naprawy. W przypadku śmigłowców

wyposażonych w dodatkowy zbiornik paliwa, ściana jest zasłonięta przez zbiornik. Z jednej oddziela on wtedy ścianę od bagażu, jednakże z drugiej strony uniemożliwia weryfikację jej stanu technicznego (uszkodzenia mogły powstać gdy dodatkowy zbiornik był zdemontowany).

Najważniejsze jest jednak zachowanie szczególnej uwagi przy załadunku i rozładunku bagażu, jak również odpowiednie zabezpieczanie go przed samoczynnym przemieszczaniem się w trakcie lotu.

**Michał Wawrzyk**  
**Senior CAMO Engineer**  
**Heli-One (Poland) Sp. z o.o.**

**Departament Zarządzania Bezpieczeństwem  
w Lotnictwie Cywilnym  
Urząd Lotnictwa Cywilnego**

ul. Marcina Flisa 2  
02-247 Warszawa

tel: + 22 520 75 22  
biuletyn@ulc.gov.pl

[www.ulc.gov.pl](http://www.ulc.gov.pl)



Urząd Lotnictwa Cywilnego