## WYTYCZNE NR 10
## PREZESA URZĘDU LOTNICTWA CYWILNEGO

z dnia 22 września 2011 r.

**w sprawie wprowadzenia do stosowania wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) – Doc 9859**

Na podstawie art. 21 ust. 2 pkt 16 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2006 r. Nr 100, poz. 696, z późn. zm.[1)]) ogłasza się, co następuje:

**§ 1.** 1. W celu realizacji norm i zalecanych metod postępowania określonych w Załączniku 1, 6, 11, 13 i 14 do Konwencji o międzynarodowym lotnictwie cywilnym, podpisanej w Chicago dnia 7 grudnia 1944 r. (Dz. U. z 1959 r. Nr 35, poz. 212 i 214, z późn. zm.[2)]), w zakresie wdrażania programów bezpieczeństwa oraz systemów zarządzania bezpieczeństwem, zaleca się stosowanie wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w Doc 9859 „Podręcznik zarządzania bezpieczeństwem" (wydanie drugie).

2. Wymagania, o których mowa w ust. 1, określa załącznik do wytycznych.

**§ 2.** Tracą moc wytyczne nr 6 Prezesa Urzędu Lotnictwa Cywilnego z dnia 24 maja 2011 r. w sprawie wprowadzenia do stosowania wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) – Doc 9859 „Podręcznik zarządzania bezpieczeństwem" (wydanie pierwsze).

**§ 3.** Wytyczne wchodzą w życie z dniem ogłoszenia.

Prezes Urzędu Lotnictwa Cywilnego
*Grzegorz Kruszyński*

---

*[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 141, poz. 1008, Nr 170, poz. 1217 i Nr 249, poz. 1829, z 2007 r. Nr 50, poz. 331 i Nr 82, poz. 558, z 2008 r. Nr 97, poz. 625, Nr 144, poz. 901, Nr 177, poz. 1095, Nr 180, poz. 1113 i Nr 227, poz. 1505, z 2009 r. Nr 18, poz. 97 i Nr 42, poz. 340, z 2010 r. Nr 47, poz. 278 i Nr 182, poz. 1228 oraz z 2011 r. Nr 80, poz. 432, Nr 106, poz. 622, Nr 170, poz. 1015 i Nr 171, poz. 1016.*

*[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 1063 r. Nr 24, poz. 137 i 138, z 1969 r. Nr 27, poz. 210 i 211, z 1976 r. Nr 21, poz. 130 i 131, Nr 32, poz. 188 i 189 i Nr 39, poz. 227 i 228, z 1984 r. Nr 39, poz. 199 i 200, z 2000 r. Nr 39, poz. 446 i 447, z 2002 r. Nr 58, poz. 527 i 528 oraz z 2003 r. Nr 78, poz. 700 i 701.*

*Załącznik do Wytycznych nr 10*
*Prezesa Urzędu Lotnictwa Cywilnego*
*z dnia 22 września 2011 r.*

**Doc 9859**
**AN/474**

# PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM

**(wydanie drugie – 2009)**

**URZĄD LOTNICTWA CYWILNEGO**

# Spis treści

# SKRÓTY I OZNACZENIA

| Skrót/Akronim | Rozwinięcie/a | Znaczenie |
|---|---|---|
| ADREP | Accident/incident Data REPorting (ICAO) | System zgłaszania Informacji o wypadkach/incydentach (do ICAO) |
| AEP | Aerodrome Emergency Plan | Plan działa w sytuacjach zagrożenia dla lotniska |
| AIRPROX | AIRcraft PROXimity | Zbliżenie statków powietrznych |
| ALARP | As Low As Reasonably Practicable | Tak niski jak to jest racjonalnie uzasadnione |
| ALoS | Acceptable Level of Safety | Akceptowalny poziom bezpieczeństwa |
| AMJ | Advisory Material Joint | Wspólne materiały doradcze |
| AMO | Approved Maintenance Organization | Zatwierdzona organizacja obsługowa |
| AOC | Air Operator Certificate | Certyfikat operatora lotniczego |
| ASDE | Airport surface detection equipment | Radar obserwacji płaszczyzny lotniska |
| ASR | Air safety report | Raport o zdarzeniu lotniczym |
| ATC | Air Traffic Control | Kontrola ruchu lotniczego |
| ATCO | Air Traffic COntroller | Kontroler ruchu lotniczego |
| ATM | Air Traffic Management | Zarządzanie ruchem lotniczym |
| ATS | Air Traffic Service(s) | Służba ruchu lotniczego |
| CAA | Civil Aviation Authority | Władze lotnictwa cywilnego |
| CDA | Continous Descent Approach | Podejście do lądowania ze stałym kątem zniżania i utrzymanie pionowego opadania |
| CEO | Chief Executive Officer | Prezes zarządu |
| CFIT | Controlled Flight Into Terrain | Zderzenie z terenem w locie kontrolowanym (bez oznak utraty kontroli nad statkiem powietrznym) |
| CIP | Commercially Important Person | Osoba bardzo ważna z handlowego punktu widzenia |
| Cir | Circular | Okólnik |
| CMC | Crisis Management Centre | Centrum zarządzania kryzysowego |
| CRDA | Converging Runway Display Aid | Oprogramowanie urządzeń radarowych wspierające operacje na zbiegających się/krzyżujących się drogach startowych |
| CRM | Crew Resource Management | Zarządzanie zasobami załogi |
| CVR | Cockpit Voice Recorder | Rejestrator głosów w kabinie |
| DME | Distance Measuring Equipment | System pomiaru odległości; Odległościomierz DME |
| Doc | Document | Podręcznik |
| ERP | Emergency Response Plan | Plan reagowania w sytuacjach zagrożenia |
| FDA | Flight data analysis | Analiza danych lotu |
| FDM | Flight data monitoring | Monitorowanie danych lotu |
| FDR | Flight Data Recorder | Rejestrator parametrów lotu |
| FOD | Foreign Object (debris) Damage | Uszkodzenie ciałem obcym (szczątkami) |
| ft | Feet | Stopa |
| GPS | Global Positioning System | Globalny system pozycjonowania |
| ILS | Instrument Landing System | System lądowania według przyrządów |
| IMC | Instrument Meteorological Conditions | Warunki meteorologiczne dla lotów według wskazań przyrządów |
| ISO | International Organization for Standardization | Międzynarodowa Organizacja Normalizacyjna |
| kg | Kilogram(s) | Kilogram |

| | | |
|---|---|---|
| LOFT | Line-Oriented Flight Training | Szkolenie symulatorowe do lotów liniowych |
| LOSA | Line Operations Safety Audit | Audyt bezpieczeństwa operatora podczas lotu operacyjnego |
| m | Metre(s) | Metr |
| MDA | Minimum descent altitude | Minimalna wysokość bezwzględna zniżania |
| MEL | Minimum Equipment List | Lista minimalnego wyposażenia |
| MOR | Mandatory Occurrence Report | Obowiązkowy system raportowania o zdarzeniach lotniczych |
| MRM | Maintenance Resource Management | Zarządzanie zasobami obsługi |
| NM | Nautical Mile(s) | Mila morska |
| OJT | On-the-Job Training | Szkolenie na stanowisku operacyjnym/w miejscu pracy |
| PC | Personal Computer | Komputer osobisty |
| QA | Quality Assurance | Zapewnienie Jakości |
| QC | Quality Control | Kontrola jakości |
| QMS | Quality Management System | System zarządzania jakością |
| RVSM | Reduced vertical separation minimum | Zmniejszone minima separacji pionowej |
| SA | Safety Assurance | Zapewnienie bezpieczeństwa |
| SAG | Safety Action Group | Grupa działań ds. bezpieczeństwa |
| SARPs | Standards And Recommended Practices (ICAO) | Normy i zalecone metody postępowania (termin ICAO) |
| SDCPS | Safety Data Collection and Processing Systems | System zbierania i przetwarzania danych dot. bezpieczeństwa |
| SHEL | Software/Hardware/Environment/Liveware | Procedury/Sprzęt/ Środowisko/Czynnik ludzki |
| SMM | Safety Management Manual | Podręcznik zarządzania bezpieczeństwem |
| SMS | Safety Management System(s) | System zarządzania bezpieczeństwem |
| SMSM | Safety Management Systems Manual | Podręcznik systemu zarządzania bezpieczeństwem |
| SOPs | Standard Operating Procedures | Standardowe procedury operacyjne |
| SRB | Safety Review Board | Komisja ds. przeglądu bezpieczeństwa |
| SRM | Safety Risk Management | Zarządzaniem ryzykiem bezpieczeństwa |
| SSP | State Safety Programme | Krajowy program bezpieczeństwa |
| TLH | Top Level Hazard | Zagrożenie najwyższego stopnia |
| TRM | Team Resource Management | Zarządzanie zasobami zespołu |
| USOAP | Universal Safety Oversight Audit Programme (ICAO) | Uniwersalny Program Nadzoru (Auditu) Bezpieczeństwa (ICAO) |
| VIP | Very Important Person | Bardzo ważna osoba |
| VMC | Visual Meteorological Conditions | Warunki meteorologiczne do lotów z widocznością |
| VOR | Very high frequency omnidirectional range | Radiolatarnia VOR |

# Rozdział 1

# PRZEGLĄD PODRĘCZNIKA

## 1.1 UWAGI OGÓLNE

Celem niniejszego podręcznika jest przedstawienie Państwom wytycznych do opracowania ram prawnych oraz zaprezentowanie materiałów pomocniczych umożliwiających dostawcom usług wdrożenie systemów zarządzania bezpieczeństwem (SMS). Podręcznik zawiera również wytyczne, ułatwiające opracowanie krajowego programu bezpieczeństwa (State Safety Programme (SSP)), zgodnie z międzynarodowymi normami i zaleconymi metodami postępowania (SARPs) zawartymi w Załącznikach: Załącznik 1 — *Licencjonowanie personelu*, Załącznik 6 — *Eksploatacja statków powietrznych*, Załącznik 8 — *Zdatność statków powietrznych*, Załącznik 11 — *Służby ruchu lotniczego*, Załącznik 13 — *Badanie wypadków i incydentów statków powietrznych*, Załącznik 14 — *Lotniska*.

## 1.2 CELE

Celem niniejszego podręcznika jest zapewnienie Państwom:

a) wiedzy o koncepcjach zarządzania bezpieczeństwem, o normach i zaleconych metodach postępowania (ICAO SARPs) dotyczących zarządzania bezpieczeństwem, zawartych w Załącznikach 1, 6, 8, 11, 13, 14 oraz w materiałach pomocniczych;

b) wytycznych do akceptowania i nadzorowania metod wdrażania kluczowych elementów systemów zarządzania bezpieczeństwem (SMS), zgodnie z odnośnymi materiałami ICAO SARPs;

c) wytycznych co do sposobu opracowania i wdrożenia krajowego programu bezpieczeństwa (SSP), zgodnie z odnośnymi normami i zaleconymi metodami postępowania ICAO SARPs.

## 1.3 KONCEPCJA

Koncepcja stanowiąca podstawę niniejszego podręcznika jest „zamkniętą pętlą” (patrz rys. 1-1). Pierwotnie, podręcznik przedstawiał podstawowe koncepcje bezpieczeństwa, stanowiące podstawę do zrozumienia potrzeby posiadania zarówno SMS, jak i SSP. W dalszej części podręcznik przedstawia sposób podejścia ICAO do koncepcji bezpieczeństwa, zawartych w normach i zaleconych metodach postępowania zawartych, które znajdują się w Załącznikach: 1, 6, 8, 11, 13 i 14.

Podręcznik przedstawia i uzasadnia sposoby wdrożenia SMS przez dostawców usług oraz dalsze wdrażanie i utrzymanie krajowego programu bezpieczeństwa (SSP), przy jednoczesnym podkreśleniu wspomagającej roli Władzy Lotniczej (CAA) w tym procesie.

## 1.4 ZAWARTOŚĆ

1.4.1 Podręcznik składa się z jedenastu poniższych rozdziałów:

a) Rozdział 1 — Przegląd podręcznika;

b) Rozdział 2 — Podstawowe koncepcje bezpieczeństwa;

c) Rozdział 3 – Wprowadzenie do zarządzania bezpieczeństwem;

d) Rozdział 4 — Zagrożenia;

e) Rozdział 5 — Ryzyko bezpieczeństwa;

f) Rozdział 6 — Wymagania ICAO dotyczące zarządzania bezpieczeństwem;

g) Rozdział 7 — Wprowadzenie do systemów zarządzania bezpieczeństwem (SMS);

h) Rozdział 8 — Planowanie SMS;

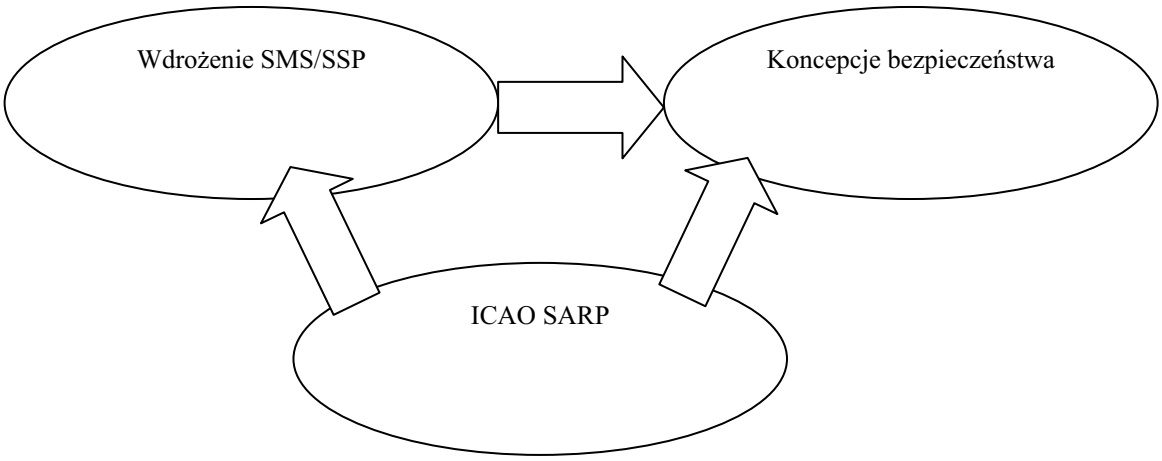
i) Rozdział 9 — Operacje SMS;

j) Rozdział 10 — Podejście etapowe do wdrożenia SMS;

k) Rozdział 11 — Krajowy program bezpieczeństwa (SSP).

1.4.2 Podręcznik zawiera również kilka „Dodatków" z praktycznymi przykładami i informacją bezpośrednio związaną z procesem wdrażania i utrzymania SMS i SSP. „Dodatki" te następują bezpośrednio po rozdziale omawiającym działania, które wspierają i należy traktować je jako wiedzę obowiązkową.

1.4.3 W podręczniku znajdują się również „Dodatki" zawierające pożyteczne informacje, niezwiązane bezpośrednio z procesem wdrażania i utrzymania SMS lub SSP. „Dodatki" te znajdują się na końcu podręcznika i należy traktować je jako materiały „warte poznania".




**Rysunek 1-1 Koncepcja zamkniętej pętli wykorzystana w podręczniku**

### 1.5 STRUKTURA

1.5.1 Podręcznik opracowany jest na zasadzie konstrukcji blokowej. Rozdział 2 ustanawia fundament poprzez omówienie współczesnych koncepcji związanych z bezpieczeństwem. Rozdział 3 wprowadza podstawy zarządzania bezpieczeństwem z podkreśleniem powodów, dla których należy zarządzać bezpieczeństwem. Rozdział 4 i 5 wprowadza szkielet dogmatyczny stanowiący podstawę do zarządzania ryzykiem i wyjaśnia dwie podstawowe koncepcje: zagrożenie i ryzyko bezpieczeństwa. I wreszcie, rozdziały od 6 do 11 omawiają i uzasadniają zasady doboru formy, metod wdrażania i utrzymania procesów zarządzania bezpieczeństwem stosując SSP i SMS jako systemy zarządzania bezpieczeństwem w Państwach i organizacjach. Rozdziały te również omawiają pojęcie zarządzania bezpieczeństwem jako czynność systematyczną.

1.5.2 Rozdział 11 omawiający krajowy program bezpieczeństwa stanowi tymczasowy materiał pomocniczy do czasu, aż ICAO i Państwa zdobędą odpowiednie doświadczenie w opracowywaniu i wdrażaniu SSP. Wówczas opracowany zostanie podręcznik poświęcony krajowemu programowi bezpieczeństwa. Dodatkowe, szczegółowe wytyczne w sprawie opracowania i wdrożenia SSP można uzyskać podczas kursu ICAO SSP Training Course, który jest dostępny na stronach: www.icao.int/fsix lub www.icao.int/anb/safetymanagement.

1.5.3 Drugie wydanie Podręcznika Zarządzania Bezpieczeństwem ICAO (SMM) (Doc 9859) zastępuje w całości pierwsze wydanie opublikowane w 2006 r. To wydanie zastępuje również Podręcznik Zapobiegania Wypadkom ICAO (Doc 9422), który staje się nieaktualny.

# Rozdział 2

# PODSTAWOWE POJĘCIA BEZPIECZEŃSTWA

## 2.1 CEL I ZAWARTOŚĆ

2.1.1 W niniejszym rozdziale przedstawiono mocne i słabe strony ugruntowanego podejścia do bezpieczeństwa oraz zaproponowano nowe perspektywy i koncepcje leżące u podstaw współczesnego podejścia do bezpieczeństwa.

2.1.2 Rozdział zawiera następujące tematy:

a) Pojęcie bezpieczeństwa;

b) Ewolucja myślenia o bezpieczeństwie;

c) Związki przyczynowe prowadzące do wypadku - model Reasona;

d) Wypadek organizacyjny;

e) Ludzie, rzeczywistość i bezpieczeństwo - model SHEL;

f) Błędy i naruszenia;

g) Kultura organizacyjna;

h) Dochodzenie/postępowanie dotyczące bezpieczeństwa.

## 2.2 POJĘCIE BEZPIECZEŃSTWA

2.2.1 W zależności od punktu widzenia, pojęcie bezpieczeństwa lotniczego może mieć różne skojarzenia, takie jak:

a) brak wypadków i poważnych incydentów - pogląd powszechnie reprezentowany przez podróżnych;

b) brak zagrożeń, czyli czynników, które powodują lub mogą powodować szkody;

c) postawa pracowników organizacji lotniczych w stosunku do niebezpiecznych działań i warunków;

d) unikanie błędów;

e) zgodność z przepisami.

2.2.2 Niezależnie od konotacji, wszystkie przedstawione elementy mają jeden wspólny mianownik: możliwość całkowitej kontroli. Brak wypadków, brak zagrożeń, itd. wskazuje ideę, że jest to możliwe (poprzez właściwy projekt lub właściwe działania), aby opanować i kontrolować wszystkie czynniki, które w lotniczej rzeczywistości operacyjnej mogą wywoływać szkodliwe skutki. Jednakże o ile eliminacja wypadków i / lub poważnych incydentów i osiągnięcie absolutnej kontroli jest z pewnością pożądane, o tyle jest to nieosiągalny cel w otwartej i podlegającej dynamicznym zmianom rzeczywistości operacyjnej. Zagrożenia są integralną częścią działalności operacyjnej. Błędy i pomyłki będą występować w lotnictwie, mimo podejmowanych wysiłków zmierzających do ich zapobiegania. Żadna działalność człowieka czy system stworzony przez niego nie może gwarantować całkowitego wykluczenia zagrożeń czy błędów w zachowaniu.

2.2.3 Bezpieczeństwo jest więc bardziej pojęciem względnym niż bezwzględnym, w którym ryzyka bezpieczeństwa wynikające ze skutków zagrożeń w rzeczywistości operacyjnej muszą być dopuszczalne w bezpiecznym z natury systemie. Kluczową kwestią nadal jest kontrola/nadzór, ale bardziej w pojęciu względnym niż absolutnym. Tak długo jak ryzyko bezpieczeństwa i możliwość wystąpienia błędów operacyjnych w działaniu utrzymywane są na rozsądnym poziomie kontroli, tak długo systemy tak otwarte na zmiany i dynamicznie im podlegające jak cywilne lotnictwo komercyjne uznaje się za bezpieczne. Innymi słowy, ryzyka bezpieczeństwa oraz błędy operacyjne w działaniu, które są kontrolowane na rozsądnym poziomie, są dopuszczalne w systemie z natury bezpiecznym.

2.2.4 Bezpieczeństwo jest coraz bardziej postrzegane jako wynik zarządzania niektórymi z procesów organizacyjnych, które mają na celu utrzymanie ryzyka bezpieczeństwa wynikającego ze skutków zagrożeń w rzeczywistości operacyjnej w ramach zorganizowanej kontroli. Dlatego też, dla celów tego podręcznika pojęcie bezpieczeństwa ma następujące znaczenie:

***Bezpieczeństwo***. Stan, w którym możliwość wystąpienia szkody wśród osób lub mienia jest zminimalizowane i utrzymuje się w ramach ciągłego procesu identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa na dopuszczalnym poziomie lub poniżej tego dopuszczalnego poziomu.

## 2.3 EWOLUCJA MYŚLENIA W KATEGORIACH BEZPIECZEŃSTWA

2.3.1 W pierwszych latach swojej działalności, lotnictwo komercyjne było regulowane oraz charakteryzowało się niskim poziomem technologii, brakiem odpowiedniej infrastruktury, ograniczonym nadzorem; niewystarczającym zrozumieniem podstawowych zagrożeń dla operacji lotniczych. Wymagania produkcji były niewspółmierne do środków i zasobów dostępnych w celu zaspokojenia takich potrzeb.

2.3.2 Według teorii systemów bezpieczeństwa, systemy produkcyjne określiły ambitne cele produkcji bez wdrażania niezbędnych środków i zasobów do ich realizacji. To spowodowało rozwój potencjału i możliwości do częstych awarii. Dlatego trudno się dziwić, że początki lotnictwa komercyjnego charakteryzowały się wysoką częstotliwością wypadków, że nadrzędnym priorytetem na początku procesu bezpieczeństwa było zapobieganie wypadkom, z tym że podstawowym środkiem profilaktycznym zapobiegania wypadkom były wnioski wysuwane dopiero po wypadku, który miał miejsce. W tych wczesnych latach badanie wypadków było bardzo trudnym zadaniem, znacznie utrudnionym wobec braku innych możliwości niż podstawowy potencjał technologiczny ówczesnych czasów.

2.3.3 Usprawnienia technologiczne (w tym w dużej mierze mające zastosowanie do badania wypadków), wraz z rozwojem odpowiedniej infrastruktury, w równej mierze co zwiększający się nadzór prawny, doprowadziły do stopniowego, ale stałego spadku ilości wypadków. W latach pięćdziesiątych lotnictwo stało się (pod względem wypadków) jednym z najbezpieczniejszych dziedzin przemysłu, ale równocześnie jednym z najbardziej poddanych surowym regulacjom prawnym.

2.3.4 Doprowadziło to do wszechobecnego przekonania, że bezpieczeństwo można zagwarantować tak długo, jak długo są przestrzegane zasady i że każde odstępstwo od zasady musi nieuchronnie doprowadzić do utraty bezpieczeństwa. Nie negując ogromnego znaczenia narzuconych odgórnie regulacji, w związku ze wzrostem ilości złożoności i rodzajów operacji lotniczych, coraz częściej mamy do czynienia z ograniczeniami znaczenia tych regulacji. Niemożliwym jest po prostu dostarczenie wytycznych dotyczących wszystkich możliwych scenariuszy operacyjnych w tak otwartym na zmiany i dynamicznie zmianom podlegającym systemie, jakim jest lotnictwo.

2.3.5 Procesy są prowadzone zgodnie z pewnymi przekonaniami. Zatem przekonanie, że zgodność z przepisami była kluczem do bezpieczeństwa w lotnictwie, początki procesów zarządzania bezpieczeństwem były oparte o badanie działań ze zgodnością z przepisami i nadzorem. Nowa filozofia procesu zarządzania bezpieczeństwem koncentrowała się na skutkach (np. wypadków i / lub poważnych incydentów) i opierała się na badaniu wypadków w celu ustalenia przyczyny, w tym również błędów technologicznych. Jeśli technologiczne błędy nie były oczywiste, zwracano uwagę na możliwość łamania zasad przez personel operacyjny.

2.3.6 Badanie wypadków miało badać zdarzenia przeszłe w celu znalezienia punktu lub punktów w łańcuchu wydarzeń, w którym ludzie, którzy przyczynili się do naruszenia bezpieczeństwa, nie zrobili tego, czego od nich oczekiwano, zrobili coś, czego nie oczekiwano lub obydwie te rzeczy naraz. W przypadku braku błędów technologicznych, badanie miało szukać niebezpiecznych ludzkich czynności operacyjnych, tj. działań i / lub zaniechań, które mogłyby być bezpośrednio związane ze skutkiem. Po tym jak takie działania / zaniechania zostały określone i z perspektywy czasu związane z naruszeniem bezpieczeństwa, nieuniknioną konsekwencją było przypisanie winy i wymierzenie kary za brak „bezpiecznego działania".

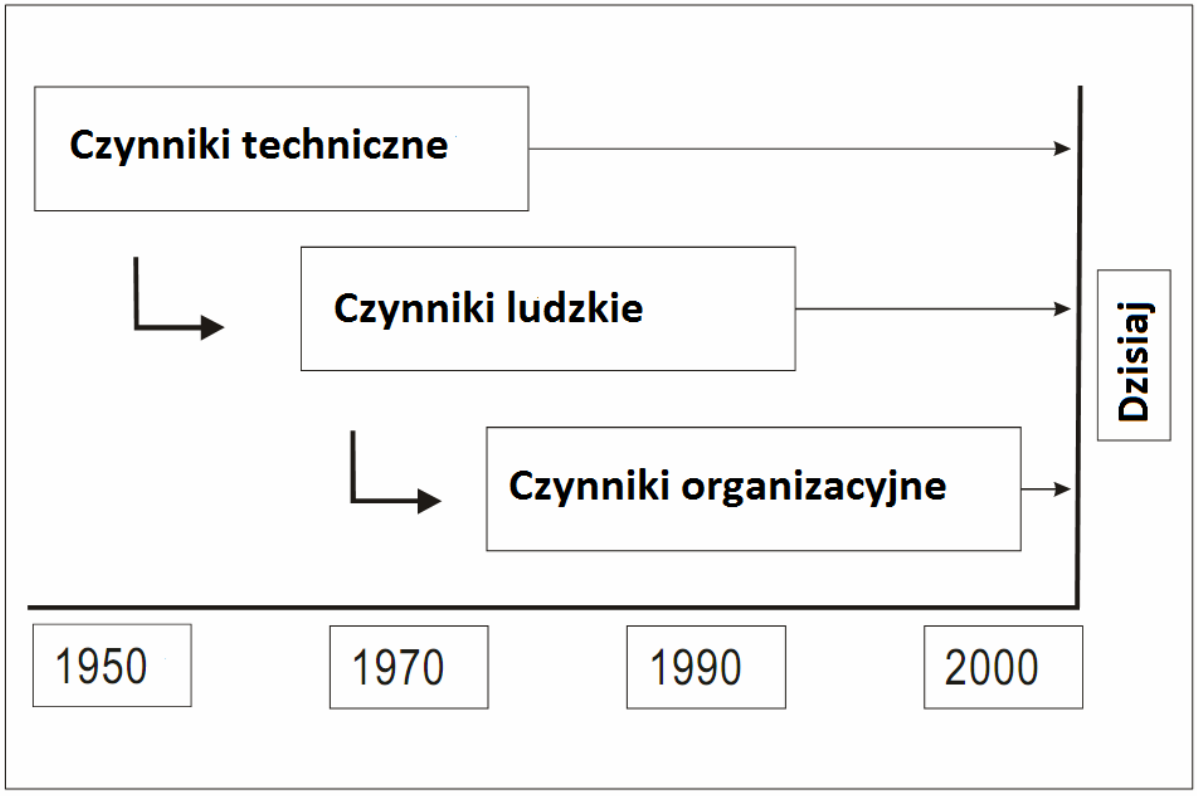
2.3.7 Typowym dla tego podejścia było wygenerowanie zaleceń bezpieczeństwa, mające na celu niemal wyłącznie tylko zabezpieczenie rzeczy wskazanej jako przyczyna naruszenia bezpieczeństwa. Tylko niewielki nacisk został położony na niebezpieczne warunki, pomimo że były potencjalnie niebezpieczne w zakresie operacji lotniczych w różnych okolicznościach. I nie były przypadkowe również dla tego zdarzenia, które zostało objęte badaniem.

2.3.8 Podczas kiedy taki punkt widzenia był bardzo skuteczny w rozpoznawaniu "co" się stało "kto" to zrobił i "kiedy" to się stało, było to znacznie mniej skuteczne w przypadku wyjaśnienia "dlaczego" i "jak" to się stało (rys. 2-1). Podczas gdy w jednym czasie było ważne, aby zrozumieć "co", "kto" i "kiedy", coraz bardziej koniecznym w celu pełnego wyjaśnienia przyczyn naruszenia bezpieczeństwa stawało się do zrozumienia "dlaczego" i "jak". W ostatnich latach dokonano znacznych postępów w realizacji tego procesu. Z perspektywy czasu oczywistym stał się fakt, że myślenie o kategoriach bezpieczeństwa lotniczego w ciągu ostatnich pięćdziesięciu lat odnotowało znaczny rozwój.


**Rysunek 2-1. Podejście tradycyjne do tematyki zapobiegania wypadkom**

2.3.9 Wczesne początki lotnictwa, które można datować przed i po II wojnie światowej, aż do lat siedemdziesiątych można scharakteryzować jako "erę techniczną." Względy bezpieczeństwa były związane głównie z czynnikami technicznymi. Lotnictwo jawiło się jako ważna gałąź branży transportowej, jednak środki techniczne z tą branżą związane nie zostały w pełni rozwinięte, a błędy technologiczne były powtarzającym się czynnikiem naruszeń bezpieczeństwa. Słusznie głównym celem badań z zakresu bezpieczeństwa było skupienie się na poprawie czynników technicznych.

2.3.10 W latach siedemdziesiątych nastąpił istotny postęp technologiczny związany z wprowadzeniem silników odrzutowych, radarów (zarówno pokładowych jak i naziemnych), funkcji autopilota, usprawnionej nawigacji i łączności oraz podobnej technologii zwiększającej wydajność, zarówno w powietrzu jak i na ziemi. Oznaczało to początek "ery człowieka", a punkt ciężkości odpowiedzialności za bezpieczeństwo przesunął się na czynnik ludzki i działalność człowieka, na zarządzanie zasobami (CRM), na zorientowane liniowo szkolenie w powietrzu (LOFT), na zorientowanej na człowieka automatyce oraz zaangażowaniu w proces innych ludzi. Okres od połowy lat siedemdziesiątych do połowy lat dziewięćdziesiątych został ochrzczony mianem "złotej ery" lotniczego czynnika ludzkiego, mającego odniesienie do dużych inwestycji podjętych przez lotnictwo do opanowania nieuchwytnego i wszechobecnego błędu ludzkiego. Niemniej jednak, pomimo ogromnych inwestycji środków w zakresie łagodzenia skutków ludzkich błędów, w połowie lat dziewięćdziesiątych działalność człowieka nadal jest wskazywana jako powtarzający się czynnik łamania bezpieczeństwa (rysunek 2-2).




**Rysunek 2-2. Ewolucja myślenia o bezpieczeństwie**

2.3.11 Wadą zajmowania się czynnikiem ludzkim podczas znacznej części "Złotej Ery" było to, że starano się skupiać na działaniach indywidualnych, bez większej uwagi na otaczającą rzeczywistość operacyjną, w ramach której te działania były podejmowane. Dopiero na początku lat dziewięćdziesiątych po raz pierwszy przyznano, że ludzie nie działają w próżni, ale w określonych sytuacjach operacyjnych. Chociaż była dostępna literatura naukowa, w której opisywano kwestie dotyczące sposobu w jaki rzeczywistość w której człowiek podejmuje działania może mieć wpływ na wydajność oraz kształt i wyniki tych działań, dopiero na początku lat dziewięćdziesiątych lotnictwo uznało to za fakt. Sygnalizuje to początek "ery organizacyjnej", w której bezpieczeństwo zaczęło być postrzegane z systemowego punktu widzenia tak, aby objąć czynniki i ludzkie, i organizacyjne, i techniczne. Był to również okres, w którym pojawiło się pojęcie wypadku lotniczego z przyczyn organizacyjnych.

## 2.4 ZWIĄZKI PRZYCZYNOWE PROWADZĄCE DO WYPADKU – MODEL REASONA

2.4.1 W całej branży, przyjęcie koncepcji wypadku z przyczyn organizacyjnych było możliwe dzięki prostemu, ale skutecznie wszystko wyjaśniającemu, modelowi opracowanemu przez profesora Jamesa Reasona, który przedstawia jak lotnictwo (lub jakikolwiek inny system produkcyjny) albo z powodzeniem działa albo ponosi porażkę. Zgodnie z tym modelem, wypadki wymagają zaistnienia kilku sprzyjających czynników - każdy z nich jest konieczny, ale jeden czynnik w pojedynkę jest niewystarczający do naruszenia systemowych linii ochrony. Ponieważ złożone systemy ochrony jakie występują w lotnictwie są bardzo dobrze bronione przez poszczególne grube warstwy tej ochrony, pojedynczy punkt awarii rzadko niesie poważne konsekwencje w systemie lotniczym. Awaria sprzętu lub błędy ludzkie w działaniu operacyjnym nigdy nie są dziurami bezpieczeństwa w ochronie, lecz jedynie aktywatorem. Dziurami bezpieczeństwa w ochronie są opóźnione w czasie konsekwencje (wyniki) decyzji podjętych wcześniej na najwyższych szczeblach systemu, które pozostają nieaktywne i ukryte aż do momentu, kiedy skutki występowania dziury w bezpieczeństwie lub niszczycielski potencjał zostanie aktywowany przez określone zestawy okoliczności operacyjnych (aktywatorów). W tych szczególnych zestawach okoliczności, ludzkie błędy lub błędy w działaniu są aktywatorami wyzwalającymi ukryte warunki sprzyjające ułatwieniu naruszenia ochrony systemu bezpieczeństwa. Koncepcja przedstawiona przez model Reasona obejmuje wszystkie wypadki jako połączenie obu warunków: aktywatorów i ukrytych dziur.

2.4.2 Błędy ludzkie w działaniu to działania lub zaniechania, w tym zwykłe błędy i naruszenia norm, które mają bezpośredni efekt negatywny. Na ogół są one widziane z perspektywy czasu, jako czynności niebezpieczne. Błędy ludzkie w działaniu są z reguły powiązane z pierwszą linią personelu (piloci, kontrolerzy ruchu lotniczego, inżynierzy, mechanicy statków powietrznych, itp.) i mogą prowadzić do skutku jakim będą rzeczywiste szkody. Pierwsza linia personelu posiada potencjał, aby przebić linie ochrony wprowadzone w celu ochrony systemu lotnictwa przez organizację, organy regulacyjne, itp. Błędy ludzkie w działaniu mogą być skutkiem normalnych błędów, lub mogą wynikać z odchyleń od określonych procedur i praktyk. Wg modelu Reasona istnieje wiele warunków, które powodują zwykłe błędy lub doprowadzają do naruszeń norm w każdej rzeczywistości operacyjnej i które to warunki mogą wpływać indywidualnie lub na cały zespół ludzi.

2.4.3 Błędy ludzkie w działaniu personelu operacyjnego mają miejsce w rzeczywistości operacyjnej, która zawiera ukryte warunki. Warunki ukryte, to warunki obecne w systemie jeszcze przed spowodowaniem szkody i objawiające się dzięki lokalnym czynnikom wyzwalającym (aktywatorom). Konsekwencje ukrytych warunków mogą pozostać nieujawnione przez dłuższy czas. Indywidualnie rozpatrując warunki ukryte, zazwyczaj nie są one postrzegane jako szkodliwe, ponieważ nie są traktowane w pierwszej kolejności jako błędy.

2.4.4 Warunki ukryte (dziury w systemie) stają się dopiero oczywiste, gdy poszczególne warstwy ochrony zostaną już naruszone. Warunki te są zazwyczaj stworzone przez ludzi, znacznie wcześniej niż samo wystąpienie zdarzenia (naruszenia). Pierwsza linia personelu operacyjnego działa niejako już w rzeczywistości, w której te dziury (warunki ukryte) istnieją. Przykładem takich warunków ukrytych mogą być: wadliwy lub nieprawidłowo zaprojektowany sprzęt, sprzeczne cele (np. usługi, w których wymagany pośpiech naraża bezpieczeństwo), wadliwe struktury organizacji (np. słaba komunikacja wewnętrzna) lub nieprawidłowe decyzje z zakresu zarządzania (np. przedłużenie resursu urządzeń).
Perspektywa bezpieczeństwa leżąca u podstaw wypadków organizacyjnych ma na celu określenie i ograniczenie właśnie tych warunków ukrytych w całym systemie, a nie jedynie podejmowanie indywidualnych i jednostkowych wysiłków skierowanych w celu zminimalizowania efektów uszkodzeń (naruszeń). Należy pamiętać, iż błędy w działaniu (naruszenia) są tylko objawami problemów bezpieczeństwa, a nie ich przyczyną.

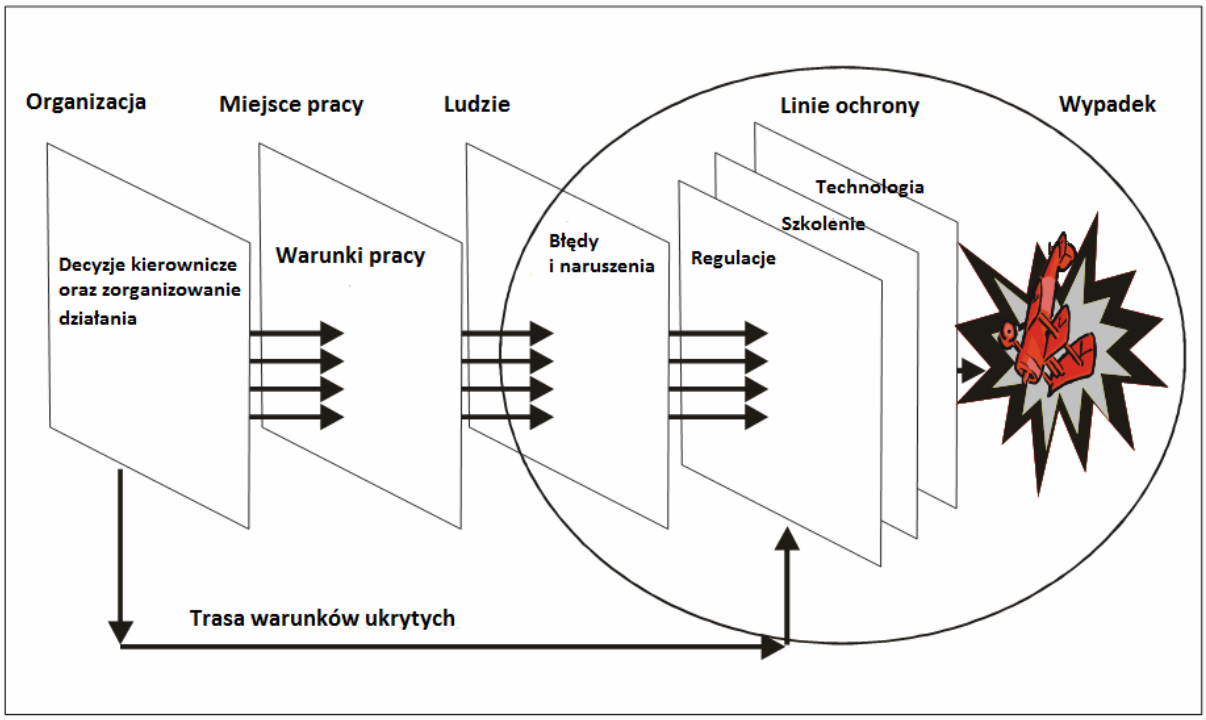
2.4.5 Nawet w najlepiej zarządzanych organizacjach, większość warunków ukrytych ma swój początek w decyzjach decydentów. Te decyzje będące decyzjami ludzkimi związane są z normalną ludzką naturą pełną pewnych uprzedzeń czy ograniczeń biologicznych, jak również związane są z pewnymi ograniczeniami rzeczywistymi takimi jak czas, budżet czy polityka. Nie zawsze można zapobiec decyzjom tworzącym dziury w systemie, należy jednak podjąć kroki, aby dziury (warunki ukryte) wykryć w porę i zmniejszyć ich negatywne skutki.

2.4.6 Decyzje kierownictwa mogą spowodować niewłaściwe wyszkolenie, nienależyte plany działań lub niewystarczające środki ostrożności. Mogą one prowadzić do braku wiedzy i umiejętności lub niewłaściwych procedur operacyjnych. W jakim stopniu kierownictwo i organizacja podczas wykonywania swoich funkcji określa margines błędów lub naruszeń? Na przykład: na ile rzeczywiste jest zarządzanie w odniesieniu do ustalonych celów pracy, zadań, organizacji i zasobów, spraw pilnych, komunikacji wewnętrznej i zewnętrznej? Decyzje podejmowane przez zarząd firmy i organy regulacyjne są zbyt często konsekwencją braku odpowiednich zasobów. Jednak unikanie początkowych kosztów na wzmocnienie bezpieczeństwa systemu może ułatwić drogę do wypadku organizacyjnego.

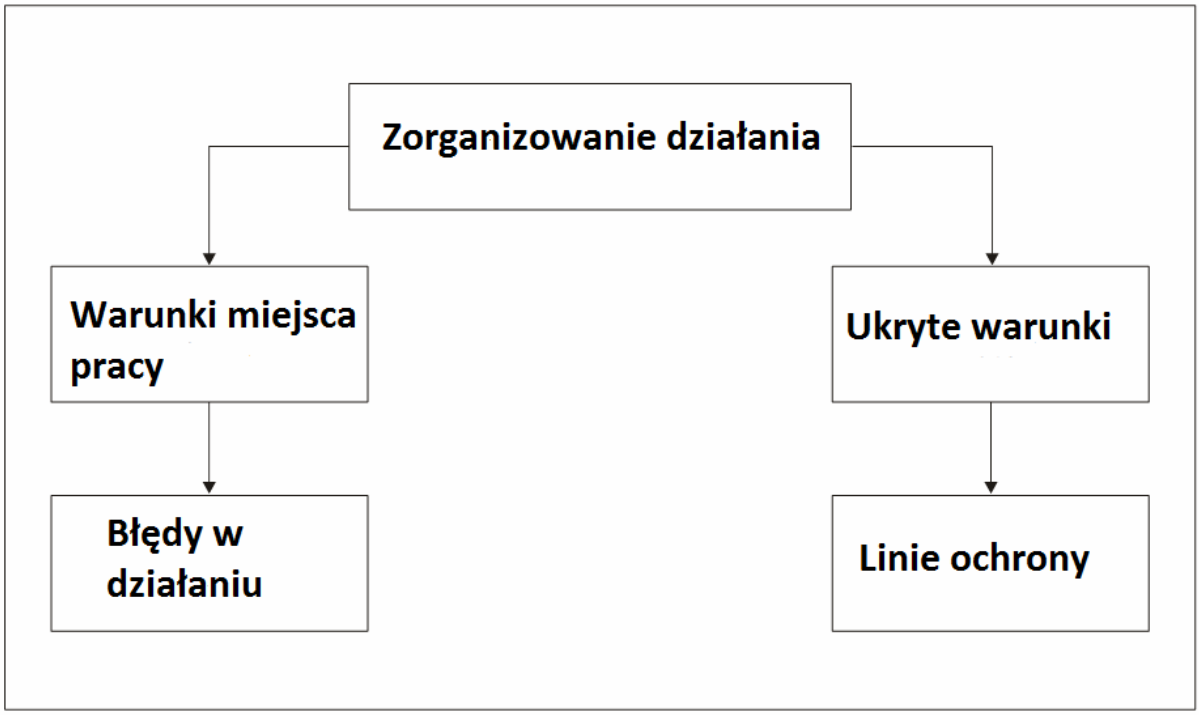
2.4.7 Rysunek 2-3 przedstawia model Reasona w sposób, który pomaga w zrozumieniu wzajemnych relacji pomiędzy czynnikami organizacyjnymi i czynnikami zarządzania (tj. czynnikami systemowymi) w związku przyczynowym wypadku. W lotnictwie na wszystkich poziomach systemu (np. miejsce pracy pierwszej linii personelu, poziom nadzoru i kierownictwa wyższego szczebla) szeroko zostały stworzone różne mechanizmy obronne (płaszczyzny ochrony) mające chronić system przed wpływem niepożądanych działań człowieka lub decyzji z negatywnym przełożeniem na bezpieczeństwo. Płaszczyzny ochrony, które muszą podlegać nieustannemu nadzorowi są środkami przewidzianymi przez system i mają chronić przed ryzykiem bezpieczeństwa, które generuje każda organizacja. Ten model pokazuje, że czynniki organizacyjne, w tym decyzje dotyczące zarządzania, mogą tworzyć zarówno warunki ukryte (dziury) w systemie, jak i przyczynić się do stabilności systemu obrony.

## 2.5 WYPADEK Z PRZYCZYN ORGANIZACYJNYCH

2.5.1 Pojęcie wypadku z przyczyn organizacyjnych opiera się na modelu Reasona i może być najlepiej rozumiane przez schemat blokowy, składający się z pięciu bloków (rys. 2-4).




**Rysunek 2-3. Koncepcja przyczyn wypadków**




**Rysunek 2-4. Wypadek organizacyjny**

2.5.2 Górny blok reprezentuje procesy organizacyjne. Są to działania, które każda organizacja wystarczająco i bezpośrednio może kontrolować. Typowe przykłady to: tworzenie polityki, planowanie, komunikacja, przydzielanie zasobów, nadzoru i tak dalej. Nie ulega wątpliwości, że dwa podstawowe procesy organizacyjne dla bezpieczeństwa to przydział zasobów i komunikacja. Wady lub braki w tych procesach organizacyjnych są początkiem podwójnej ścieżki prowadzącej do porażki.

2.5.3 Pierwszą ścieżką jest ścieżka warunków ukrytych (dziur). Przykłady dziur mogą obejmować: braki w konstrukcji urządzeń, niepełne / nieprawidłowe standardy procedur operacyjnych i braki w zakresie szkolenia. W sposób ogólny, warunki ukryte można podzielić na dwie grupy. Jedna grupa to niewystarczająca identyfikacja zagrożeń i nieprawidłowe zarządzanie ryzykiem, w której ryzyko bezpieczeństwa jako konsekwencja zagrożeń nie jest utrzymywane pod kontrolą, ale swobodnie porusza się w systemie, aby w końcu uaktywnić się poprzez aktywatory działania operacyjnego.

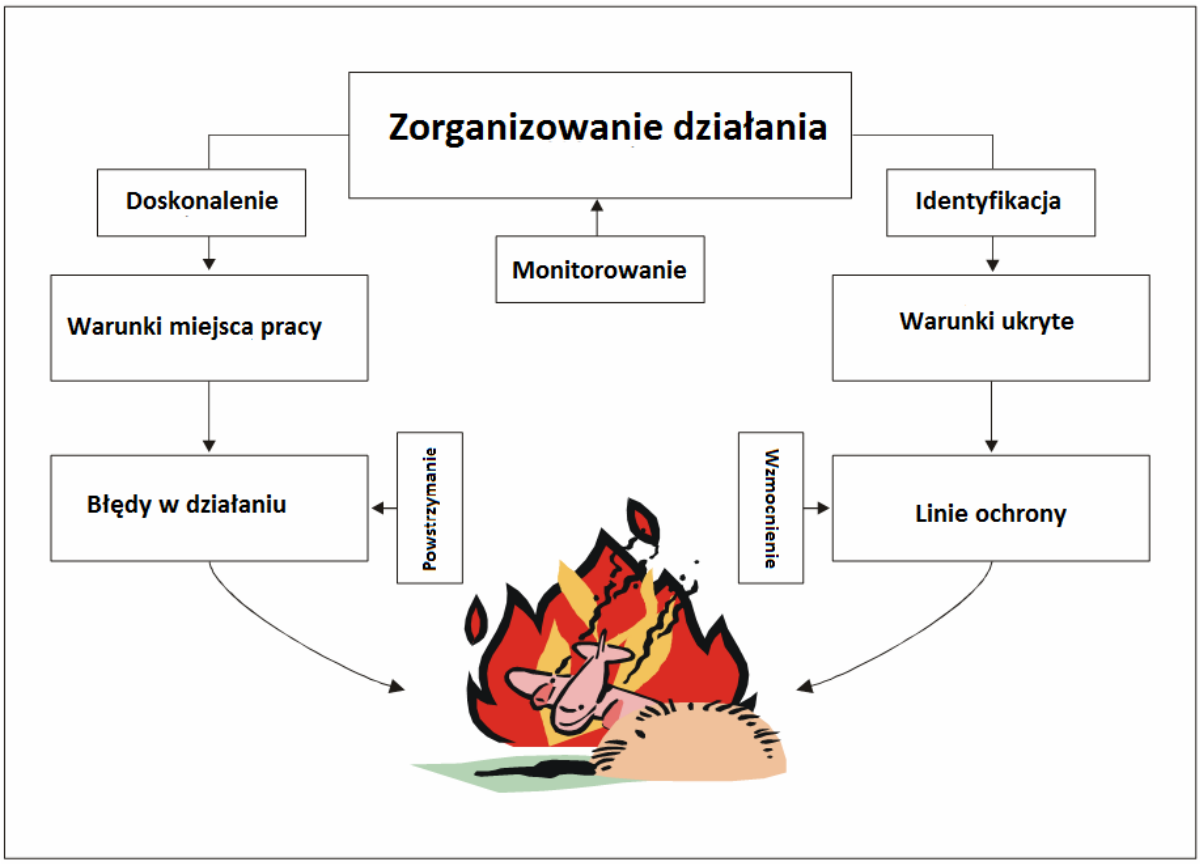
2.5.4 Drugi obszar jest znany jako normalizacja odchyleń. Pojęcie, które wskazuje na rzeczywistość operacyjną, w której wyjątki stają się regułami. Alokacja zasobów w tym przypadku jest ekstremalnie wadliwa. W związku z brakiem środków oraz możliwości, jedynym sposobem osiągnięcia celu dla personelu operacyjnego, który jest bezpośrednio odpowiedzialny za faktyczne wyniki, jest stałe „chodzenie na skróty," czyli nieustanne naruszanie zasad i procedur.

2.5.5 Warunki ukryte posiadają cały potencjał do naruszenia płaszczyzn ochrony systemu lotnictwa. Zazwyczaj płaszczyzny ochrony w lotnictwie można podzielić na trzy duże grupy: technologia, szkolenia i przepisy. Płaszczyzny ochrony są zwykle ostatnimi punktami, które mają zahamować skutki warunków ukrytych (dziur), jak również konsekwencji błędów ludzkich. Większość, jeśli nie wszystkie, strategii łagodzenia ryzyka konsekwencji ryzyka bezpieczeństwa oparta jest na wzmocnieniu istniejących lub na rozwoju nowych płaszczyzn ochrony.

2.5.6 Inną ścieżką wywodzącą się z procesów organizacyjnych jest ścieżka warunków miejsca pracy. Warunki miejsca pracy są czynnikami, które bezpośrednio wpływają na wydajność pracy osób w lotnictwie. Warunki miejsca pracy są w dużej mierze intuicyjne, ale wszyscy z doświadczeniem operacyjnym w jakimś stopniu ich doświadczają i warunki te obejmują zarówno stabilność zatrudnienia, kwalifikacje i doświadczenie, morale, zaufanie do zarządzających. Również tradycyjne czynniki ergonomiczne takie jak oświetlenie, ogrzewanie i chłodzenie.

2.5.7 Warunki miejsca pracy gorsze niż optymalne sprzyjają porażkom w działaniu personelu operacyjnego. Za porażki w działaniu należy uznać zarówno błędy jak i wykroczenia. Różnicą między błędami a wykroczeniami jest element motywacyjny. Osoba, która stara się wykonać zadanie jak najlepiej, ale zgodnie z zasadami i procedurami i wg szkolenia, które otrzymała, ale nie osiąga założeń zadania popełnia gdzieś błąd. Osoba, która chętnie odbiega od zasad, procedur lub szkolenia podczas realizacji zadania, popełnia wykroczenie. Tak więc zasadniczą różnicą między błędami a wykroczeniami jest zamiar przy podjęciu działania.

2.5.8 Z perspektywy organizacyjnej wypadku, starania poprawy bezpieczeństwa powinny monitorować procesy organizacyjne w celu wykrycia warunków w formie ukrytej i tym samym wzmocnienia płaszczyzny ochrony. Starania poprawy bezpieczeństwa powinny również dotyczyć poprawy warunków miejsca pracy obciążonych błędami w działaniu, ponieważ związek tych wszystkich czynników odpowiada za łamanie bezpieczeństwa (rys. 2-5).




**Rysunek 2-5. Postrzeganie wypadku organizacyjnego**

## 2.6 LUDZIE, RZECZYWISTOŚĆ I BEZPIECZEŃSTWO - MODEL SHEL

2.6.1 Lotnicze miejsca pracy to wieloskładnikowy, multifunkcyjny zbiór rzeczywistości operacyjnych. Ich zadania i wydajność, obejmujące skomplikowane relacje między wieloma elementami, służą systemowi do osiągnięcia celów produkcyjnych.

2.6.2 Aby zrozumieć wkład człowieka w bezpieczeństwo i rozwijać wyniki operacyjne konieczne do osiągnięcia celów systemu produkcji, koniecznym jest zrozumienie w jaki sposób ludzkie wyniki operacyjne mogą dotyczyć różnych elementów i cech rzeczywistości operacyjnej oraz powiązań między jej elementami a ludźmi.

2.6.3 Bardzo prosty przykład został przedstawiony na rys. 2-6. Jaskiniowiec jest przykładem personelu operacyjnego, a misją (lub celem produkcji układu) jest dostarczanie paczek na drugą stronę gór. Zarówno różne elementy, jak i cechy rzeczywistości operacyjnej i ich interakcje z jaskiniowcem oraz między sobą, będą miały wpływ na bezpieczeństwo i efektywność dostarczania paczek. Na przykład interakcja jaskiniowca z lwami może mieć szkodliwe skutki dla dostawy paczek, chyba że jaskiniowiec jest odpowiednio wyposażony do radzenia sobie z lwami.


**Rysunek 2-6. Ludzie i bezpieczeństwo**

2.6.4 Przejście gór prawdopodobnie okrężną i nieutwardzoną drogą, bez obuwia, obniży efektywność skutecznego działania (opóźnienia w dostarczaniu paczek) i może prowadzić do obrażeń ciała, co oznacza wzrost obaw w zakresie bezpieczeństwa. Odważenie się na wyprawę bez brania pod uwagę pogody, a tym samym bez zabezpieczenia na wypadek deszczu jest również źródłem potencjalnych uchybień w zakresie bezpieczeństwa i skuteczności.

2.6.5 Jest zatem oczywiste, że właściwa ocena i analiza rzeczywistości jest źródłem cennych informacji w celu zrozumienia przygotowania operacyjnego do jego wspierania i wzmocnienia.

2.6.6 Potrzeba zrozumienia przygotowania operacyjnego i rzeczywistości jest dodatkowo zilustrowana na kolejnym przykładzie (rys.2-7A).

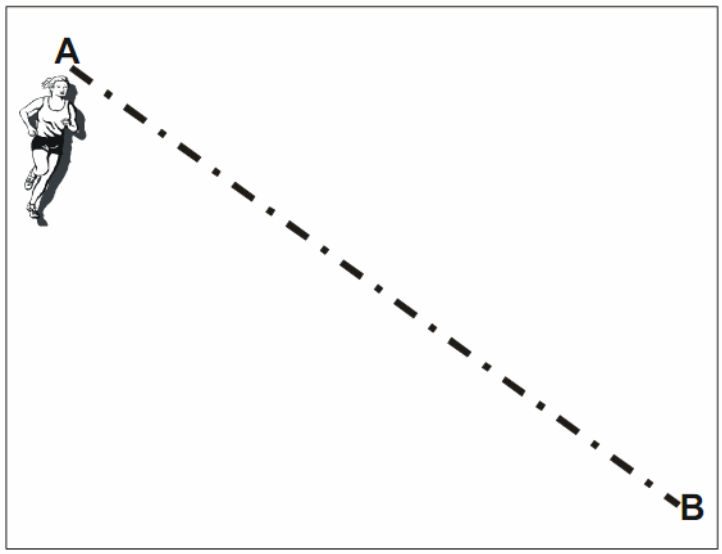
2.6.7 W tym przypadku celem systemu jest dostarczanie paczek przez zawodników pomiędzy punktami A i B. Przy podstawowym założeniu w trakcie projektowania systemu, będzie się biegać najkrótszą trasą, która jest przedstawiona w linii prostej.

2.6.8 Nie oszczędzono na inwestycjach aby optymalnie wykorzystać zasoby systemu. Najlepsze dostępne zasoby ludzkie, w tym przypadku biegacze, są wybierani, wyszkoleni, zaangażowani i wyposażeni w najlepszy dostępny sprzęt. Częścią systemu jest monitorowanie działań w czasie rzeczywistym. Po etapie poszczególnych kroków projektowanie zostało zakończone, operacja zaczyna się. Tuż po rozlokowaniu systemu, zaczyna się monitorowanie działań w czasie rzeczywistym. Ku przerażeniu administratorów systemu, monitorowanie w czasie rzeczywistym wykazuje, że większość biegaczy nie stosuje się do zamierzonego toru, wzdłuż linii prostej, ale raczej podąża drogą zygzakiem. W związku z tym dochodzi do opóźnień w dostawie, a także występują wypadki (rys. 2-7B).

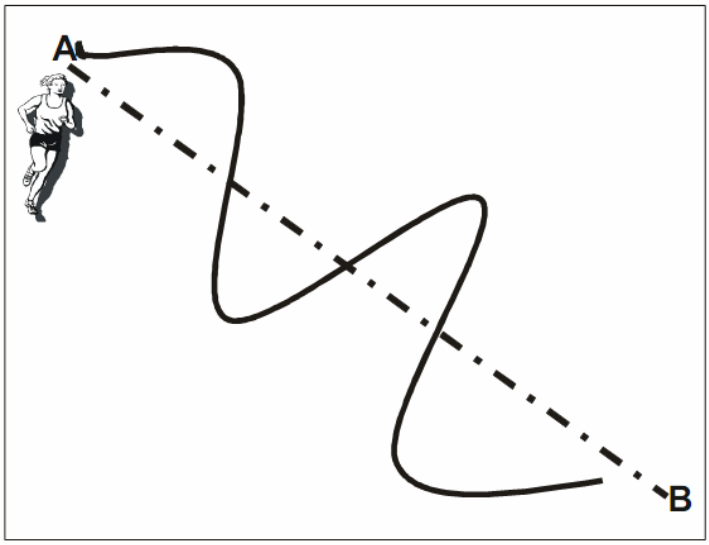
2.6.9 W tym momencie administratorzy systemu mogą wybrać dwie opcje. Jedną jest postępowanie wg tradycyjnego punktu widzenia, omówione w 2.3.6 - produkowanie „pustych" zaleceń dla biegaczy, mówiących o tym, co znają i do czego są przeszkoleni oraz obarczanie winą i karanie zawodników za działanie niezgodne z oczekiwaniami. Drugą opcją jest analiza rzeczywistości, aby zobaczyć czy występują składniki i cechy rzeczywistości, które mogą być źródłem niepożądanych interakcji z biegaczami. W przypadku drugiej opcji, zostaną nabyte cenne informacje na temat niektórych elementów i cech występujących w rzeczywistości (rys. 2-7C), które pozwolą na modyfikację założeń projektowych oraz przyczynią się do rozwoju strategii ograniczania ryzyka dla konsekwencji nieprzewidzianych elementów i cech rzeczywistości. Innymi słowy, poprzez pozyskanie informacji na temat zagrożeń (omówione w rozdziale 4) w rzeczywistości i zrozumienie ich interakcji z ludźmi, administratorzy systemu mogą przywrócić stan pierwotny systemu w ramach kontroli organizacyjnej.

2.6.10 A zatem właściwe zrozumienie przygotowań operacyjnych oraz błędów operacyjnych nie może zostać osiągnięte bez właściwego rozpoznania rzeczywistości, w której wyniki operacyjne i błędy mają miejsce. Takie rozpoznanie nie może być osiągnięte, dopóki nie zacznie się wyraźnie rozróżniać procesów i ich wyników. Istnieje tendencja do przyznania regularności przyczynom i skutkom błędów operacyjnych, która w rzeczywistości nie istnieje. Ten sam błąd może mieć znacząco różne konsekwencje, w zależności od rzeczywistości, w której ma miejsce. Konsekwencje błędów operacyjnych nie są zależne od osoby, ale od rzeczywistości (rys. 2-8). Koncepcja ta ma znaczący wpływ na strategię łagodzenia skutków: skuteczne i efektywne strategie łagodzenia skutków błędów mają na celu zmianę tych cech i komponentów rzeczywistości, które zwiększają konsekwencje błędów, a nie polegają na zmianie ludzi.

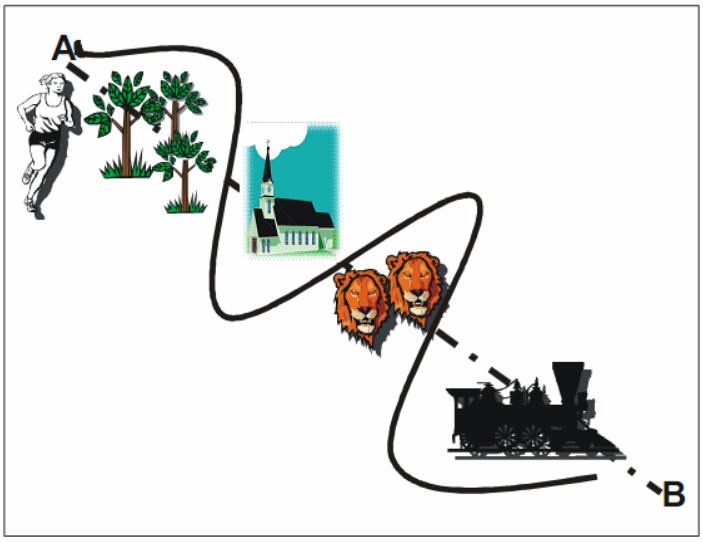
2.6.11 Rysunek 2-8 ilustruje scenariusz, w którym dwie opcje omówione w 2.3.6 mogą być zastosowane. W tradycyjnym podejściu prowadziłoby to do: przypomnienia na co zwracać uwagę, gdy człowiek opiera się o parapet okna (lub po prostu: nie opierać się o parapet) i jakie grożą niebezpieczeństwa wypchnięcia doniczki przez okno; ponownego pisania procedur, a nawet kara za wypchnięcie doniczki z okna (czyli zachowanie niezgodnie z oczekiwaniami lub niebezpiecznym wykonaniem czynności opierania sie o parapet).
Z drugiej strony, podejście organizacyjne doprowadzi do założenia siatki pod oknem, rozszerzenia parapetów, używania doniczek kruchego typu, zmiany trasy ruchu pod oknem lub w skrajnych przypadkach ogrodzenia okna. Najważniejszym celem jest to, żeby usuwając lub modyfikując cechy rzeczywistości, które mogą ułatwiać wykonanie czynności niebezpiecznej, osiągnąć cel jakim jest istotne zmniejszenie prawdopodobieństwa oraz potencjału ewentualnych zniszczeń.




**Rysunek 2-7A. Zrozumienie ludzkich zachowań**




**Rysunek 2-7B. Zrozumienie ludzkich zachowań**




**Rysunek 2-7C. Zrozumienie ludzkich zachowań**


**Rysunek 2-8. Procedury i ich rezultaty**

2.6.12 Prostym, choć silnym wizualnie narzędziem koncepcyjnym do analizy składników i cech kontekstów operacyjnych oraz ich możliwych interakcji z ludźmi jest model SHEL. Model SHEL (czasem określany jako SHEL(L)) może posłużyć do wizualizowania relacji pomiędzy różnymi składnikami i cechami systemu lotnictwa. Model ten kładzie nacisk na indywidualne i ludzkie punkty styku z innymi składnikami i cechami systemu lotnictwa. Nazwa modelu SHEL wywodzi się od początkowych liter jego czterech składników:

a) Oprogramowanie (S) [ang. „Software”] (procedury, szkolenia, wsparcie, itp.);

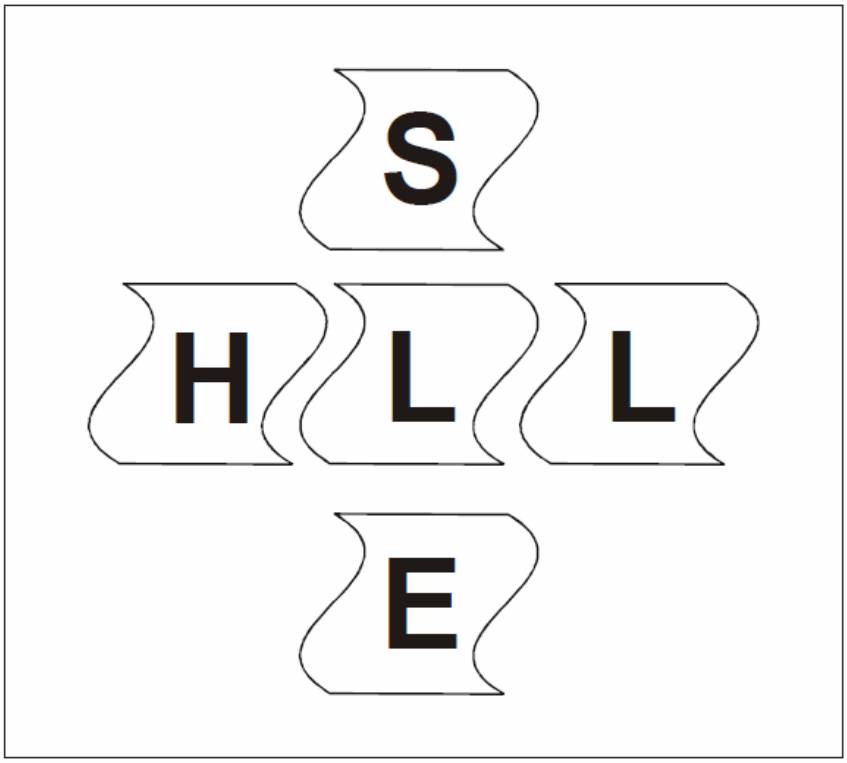
b) Sprzęt (H) [ang. „Hardware”] (maszyny i wyposażenie);

c) Środowisko (E) [ang. „Environment”] (kontekst operacyjny, w którym funkcjonuje system L-H-S);

d) Czynnik ludzki (L) [ang. „Liveware”] (ludzie w miejscu pracy).

2.6.13 Rysunek 2-9 opisuje model SHEL. Ten diagram blokowy ma na celu wyjaśnienie relacji osób ze składnikami i cechami miejsca pracy.

2.6.14 ***Czynnik ludzki.*** W centrum modelu SHEL znajdują się ludzie bezpośrednio zaangażowani w operacje. Chociaż ludzie dostosowują się bardzo dobrze, wykazują znaczne zróżnicowanie w wykonywaniu pracy. Ludzie nie są wystandaryzowani w tym samym stopniu co sprzęt, więc krawędzie tego bloku nie są równe i proste. Nie do końca też idealnie oddziałują z różnymi składnikami środowiska, w którym pracują. Aby uniknąć napięć mogących wpłynąć negatywnie na wykonywaną pracę, należy zrozumieć skutki zakłóceń na styku różnych bloków SHEL i środkowego bloku czynnik ludzki. Pozostałe składniki systemu należy starannie dopasować do ludzi, aby uniknąć napięć w systemie.




**Rysunek 2-9. Model SHEL**

2.6.15 Kilka różnych czynników sprawiło, że blok „Czynnik ludzki” ma nierówne krawędzie. Poniżej wymieniono niektóre istotniejsze czynniki wpływające na indywidualną jakość pracy:

a) ***Czynniki fizyczne***. Obejmują one fizyczne zdolności osoby do wykonywania wymaganych zadań, np. siła, wzrost, zasięg rąk, wzrok i słuch.

b) ***Czynniki fizjologiczne***. Obejmują one te czynniki wpływające na wewnętrzne procesy fizyczne osoby, które z kolei mogą pogorszyć zdolności fizyczne i poznawcze, np. dostępność tlenu, ogólne zdrowie i sprawność, choroby, tytoń, zażywanie narkotyków lub alkoholu, osobisty stres, zmęczenie i ciąża.

c) ***Czynniki psychologiczne***. Obejmują one te czynniki, które wpływają na psychologiczne przygotowanie osoby na wszelkie możliwe okoliczności, np. prawidłowość szkolenia, wiedza, doświadczenie czy obciążenie pracą.

d) ***Czynniki psychospołeczne***. Obejmują one wszelkie czynniki zewnętrzne w systemie społecznym, w którym funkcjonuje jednostka, wywierające na nią wpływ w pracy i poza pracą, np. sprzeczka z przełożonym, konflikty zarządu ze związkami zawodowymi, śmierć w rodzinie, osobiste problemy finansowe lub inne napięcia w gospodarstwie domowym.

2.6.16 Model SHEL jest szczególnie przydatny przy wizualizowaniu współoddziaływania pomiędzy różnymi składnikami systemu lotniczego. Obejmują one:

a) ***Czynnik ludzki-sprzęt (L-H)***. Styk pomiędzy człowiekiem i techniką jest najczęściej wspominany, gdy mowa o sprawności człowieka. Określa, jak człowiek współoddziałuje z fizycznym otoczeniem w miejscu pracy, np. projektowanie siedzeń w celu dostosowania do charakterystyki ludzkiego ciała, wyświetlacze dostosowane do charakterystyki zmysłów i zdolności do przetwarzania informacji przez użytkownika oraz właściwe ruchy, kodowanie i rozmieszczenie mechanizmów kontrolnych użytkownika. Jednakże istnieje naturalna, ludzka tendencja do przystosowywania się do niedopasowań L-H. Tendencja ta może przesłaniać poważne mankamenty, które mogą ujawnić się dopiero po zdarzeniu lotniczym.

b) ***Czynnik ludzki-oprogramowanie (L-S)***. Linia styku L-S to relacja pomiędzy człowiekiem a systemami wsparcia w miejscu pracy, np. regulacjami, podręcznikami, listami kontrolnymi, publikacjami, instrukcjami operacyjnymi i oprogramowaniem komputerowym. Uwzględnia to takie sprawy z zakresu „przyjazności wobec użytkownika" jak: aktualność, właściwość, format, prezentacja, słownictwo, jasność i symbolika.

c) ***Czynnik ludzki-czynnik ludzki (L-L)***. Linia styku L-L to relacja pomiędzy człowiekiem a innymi osobami w miejscu pracy. Załogi, kontrolerzy ruchu lotniczego, mechanicy obsługi statków powietrznych i inny personel operacyjny funkcjonują jako grupy, a wpływy grupowe oddziałują na wyniki pracy człowieka. Pojawienie się zarządzania zasobami załogi (CRM) stało się przedmiotem znacznego zainteresowania tymi relacjami. Szkolenie z CRM i rozszerzenie go na służby ruchu lotniczego (ATS) (zarządzanie zasobami zespołu (TRM)) i obsługę techniczną (zarządzanie zasobami obsługi (MRM)) skupiają się na zarządzaniu błędami operacyjnymi. Stosunki pracowników z kierownictwem również znajdują się w zakresie tej relacji, gdyż kultura korporacyjna, klimat panujący w firmie i napięcia wynikające z jej działalności mogą w znacznym stopniu wpłynąć na jakość pracy wykonywanej przez ludzi.

d) ***Czynnik ludzki-środowisko (L-E)***. Ta linia styku zawiera w sobie relację pomiędzy człowiekiem a środowiskiem wewnętrznym i zewnętrznym. Wewnętrzne środowisko miejsca pracy obejmuje takie warunki fizyczne jak: temperaturę, oświetlenie, hałas, wibracje i jakość powietrza. Zewnętrzne środowisko obejmuje takie aspekty jak: widoczność, turbulencję i ukształtowanie terenu. Środowisko pracy w lotnictwie 24 godziny na dobę, siedem dni w tygodniu zawiera w sobie zakłócenia normalnych rytmów biologicznych, np. rytmu snu. Ponadto system lotniczy funkcjonuje w kontekście szeroko rozumianych ograniczeń politycznych i społecznych, które z kolei wpływają na ogólne środowisko korporacyjne. Uwzględnione są tu takie czynniki jak: adekwatność wyposażenia i infrastruktury pomocniczej, lokalna sytuacja finansowa i skuteczność regulacji. Tak jak najbliższe środowisko pracy może wywierać presję na „pójście na skróty", tak nieodpowiednia infrastruktura może negatywnie wpłynąć na jakość podejmowanych decyzji.

2.6.17 Należy uważać aby błędy operacyjne nie „wcisnęły się przez szczelinę w drzwiach" na liniach styku. W większości przypadków nierówne krawędzie tych linii styku są do opanowania, np.:

a) Projektant może zapewnić niezawodność wyposażenia w określonych warunkach operacyjnych.

b) W procesie certyfikacji instytucja regulacyjna może określić realistyczne warunki, w których wyposażenie może być używane.

c) Zarząd organizacji może opracować standardowe procedury operacyjne (SOP) i zorganizować szkolenie początkowe i odświeżające z bezpiecznego użytkowania wyposażenia.

d) Poszczególni użytkownicy wyposażenia mogą upewnić się co do znajomości i zaufania do wyposażenia we wszystkich wymaganych warunkach operacyjnych.

## 2.7 BŁĘDY I NARUSZENIA

### Błędy operacyjne

2.7.1 Wzrost sektora lotniczego nie byłby możliwy gdyby nie było zaawansowanej techniki wspierającej rosnący popyt na usługi. W sektorach intensywnej produkcji (wykonywania usług) takich jak współczesne lotnictwo, technika jest niezbędna do spełnienia wymagań dotyczących świadczenia usług. Jest to podstawowa sprawa często pomijana przy analizach bezpieczeństwa. Wprowadzenie rozwiązań technicznych nie ma na celu w pierwszym rzędzie poprawy bezpieczeństwa, jego celem jest zaspokojenie popytu na zwiększoną skalę świadczenia usług przy zachowaniu dotychczasowych marginesów bezpieczeństwa.

2.7.2 Technika jest więc wprowadzana na skalę masową w celu zaspokojenia popytu na produkcję. Jednym z efektów masowego wprowadzania techniki mającej na celu poprawę świadczonych usług, jest pomijanie linii styku pomiędzy czynnikiem ludzkim a sprzętem w modelu SHEL lub też nie zawsze uwzględnia się ją tak jak się powinno. W rezultacie, niedostatecznie rozwinięta technika może być wprowadzona przedwcześnie, co prowadzić może do niespodziewanych awarii.

2.7.3 Chociaż wprowadzenie niedopracowanych rozwiązań technicznych jest nieuniknioną konsekwencją potrzeb każdego sektora masowej produkcji, jego znaczenie dla zarządzania bezpieczeństwem nie może być pomijane. Osoby na pierwszej linii, np. personel operacyjny, na co dzień stykają się z rozwiązaniami technicznymi przy wykonywaniu zadań mających na celu świadczenie usługi. Jeżeli linia styku sprzętu z czynnikiem ludzkim nie została w odpowiedni sposób uwzględniona przy tworzeniu rozwiązań technicznych i jeśli pominięto konsekwencje operacyjne kontaktów pomiędzy ludźmi a techniką, efekt jest oczywisty: błędy operacyjne.

2.7.4 Wizja błędów operacyjnych jako ujawniającej się cechy systemów łączących ludzi i urządzenia, daje znacząco odmienną perspektywę w zarządzaniu bezpieczeństwem w porównaniu z tradycyjną, opartą na psychologii, wizją błędów operacyjnych. Zgodnie z wizją opartą na psychologii źródło błędów „znajduje się" w osobie i jest konsekwencją specyficznych mechanizmów psychospołecznych badanych i wyjaśnianych przez różne dziedziny psychologii badawczej i stosowanej.

2.7.5 Próby skutecznego uprzedzania i ograniczania błędów operacyjnych według wizji opartej na psychologii są niezwykle trudne, wręcz nie całkiem niemożliwe. Przy selekcji można odrzucić osoby bez podstawowych cech charakteru wymaganych do pracy, a na zachowania można wpłynąć poprzez szkolenia i regulacje. Jednakże wada tej wizji, z czysto operacyjnego punktu widzenia, jest jasna: niemożliwym jest przewidzieć w sposób systematyczny typowe ludzkie słabości takie jak nieuwaga, zmęczenie czy roztargnienie i tego jak będą one współoddziaływać ze składnikami i cechami kontekstu operacyjnego w specyficznych warunkach operacyjnych. Indywidualne strategie ograniczania uważa się za „miękkie" ograniczanie, gdyż niedociągnięcia w sposobie wykonywania pracy przez człowieka „wyskoczą" wtedy, kiedy są najmniej spodziewane, niekoniecznie w sytuacjach trudnych i ujawnią swój niszczycielski potencjał.

2.7.6 Wizja błędów operacyjnych jako ujawniającej się cechy systemów łączących ludzi i urządzenia, usuwa człowieka jako źródło błędu operacyjnego i umieszcza to źródło całkowicie w fizycznym świecie, na styku L/H. Rozbieżność na tej linii styku jest źródłem błędu operacyjnego. Jako część świata fizycznego, źródło błędu operacyjnego staje się więc widoczne i może być wyrażone w terminach operacyjnych (przełącznik jest częściowo zasłaniany przez dźwignię, co sprawia, że trudno jest obserwować jego położenie w nocy) w odróżnieniu od terminów naukowych (ograniczenia percepcji wzrokowej). Źródło błędu operacyjnego może więc być dostrzeżone wcześniej i ograniczone poprzez interwencje operacyjne. Zarządzanie bezpieczeństwem niewiele może pomóc na ograniczenia percepcji, ale istnieje cały wachlarz opcji przeciwdziałania konsekwencjom układu z częściowo zasłoniętym przełącznikiem, dostępnych dzięki zarządzaniu bezpieczeństwem.

2.7.7 Nieodłączną częścią tradycji bezpieczeństwa w lotnictwie jest uważanie błędów operacyjnych jako czynnika sprzyjającego większości zdarzeń lotniczych. Ten oparty na perspektywie psychologicznej pogląd przedstawia błędy operacyjne jako formy zachowania, które personel operacyjny dobrowolnie przejawia, tak jakby personel operacyjny miał jasny wybór pomiędzy popełnieniem błędu operacyjnego a niepopełnieniem i dobrowolnie wybierał pierwszą opcję. Co więcej, błąd operacyjny uważany jest za wskazujący na niższą od standardowej jakość wykonywanej pracy, wady charakteru, brak profesjonalizmu, dyscypliny itp., wytworzony przez lata jedynie częściowego zrozumienia wykonywania pracy przez ludzi.

2.7.8 Kiedy zastosuje się alternatywną wizję błędów operacyjnych omówioną powyżej, uważając te błędy za ujawniającą się cechę systemów łączących ludzi i urządzenia i zlokalizuje źródło błędów w niedopasowaniu na linii styku L/H, stanie się jasnym, że nawet najbardziej kompetentny personel może popełnić błędy operacyjne.

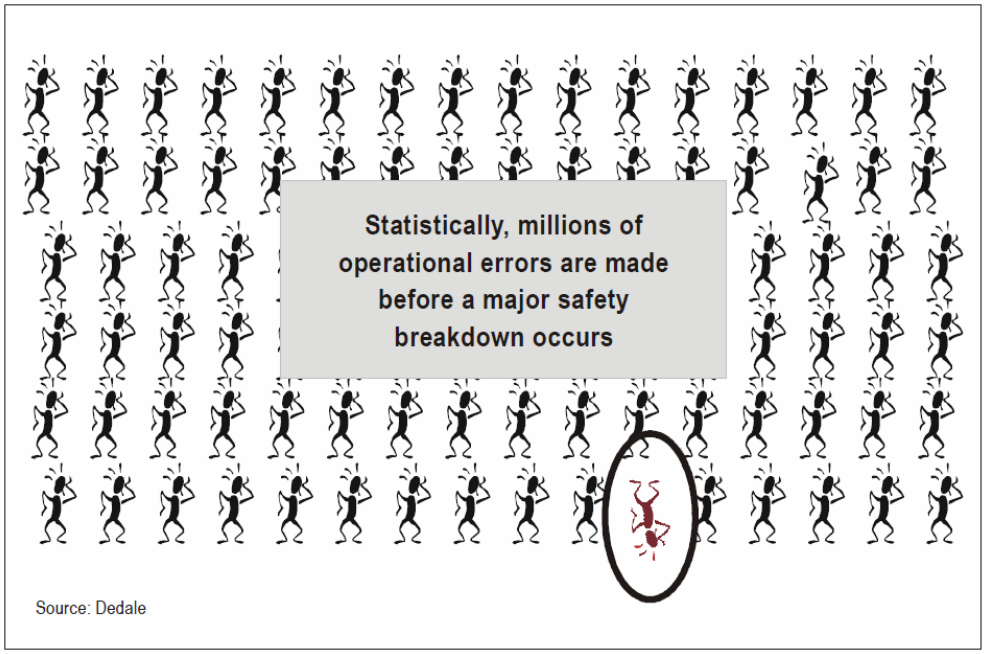
Błędy operacyjne są więc akceptowane jako normalny składnik każdego systemu, w którym oddziałują na siebie ludzie i urządzenia i nie są uważane za niespodziewane zachowanie. Błędy można postrzegać raczej jako naturalne efekty uboczne interakcji ludzi z urządzeniami podczas działań operacyjnych mających na celu świadczenie usług w dowolnym systemie produkcyjnym. Błędy operacyjne akceptowane są jako normalny składnik systemu, w którym oddziałują na siebie ludzie i urządzenia, a operacyjne strategie bezpieczeństwa są wdrażane w celu zachowania kontroli nad błędami operacyjnymi.

2.7.9 Biorąc pod uwagę nieuniknioność niedopasowań na liniach styku modelu SHEL w operacjach lotniczych, potencjalny zakres błędów operacyjnych jest ogromny. Zrozumienie, jak te niedopasowania mogą wpłynąć na przeciętnego człowieka w miejscu pracy, ma fundamentalne znaczenie dla zarządzania bezpieczeństwem. Tylko wtedy można wdrożyć skuteczne mechanizmy kontroli skutków błędów operacyjnych.

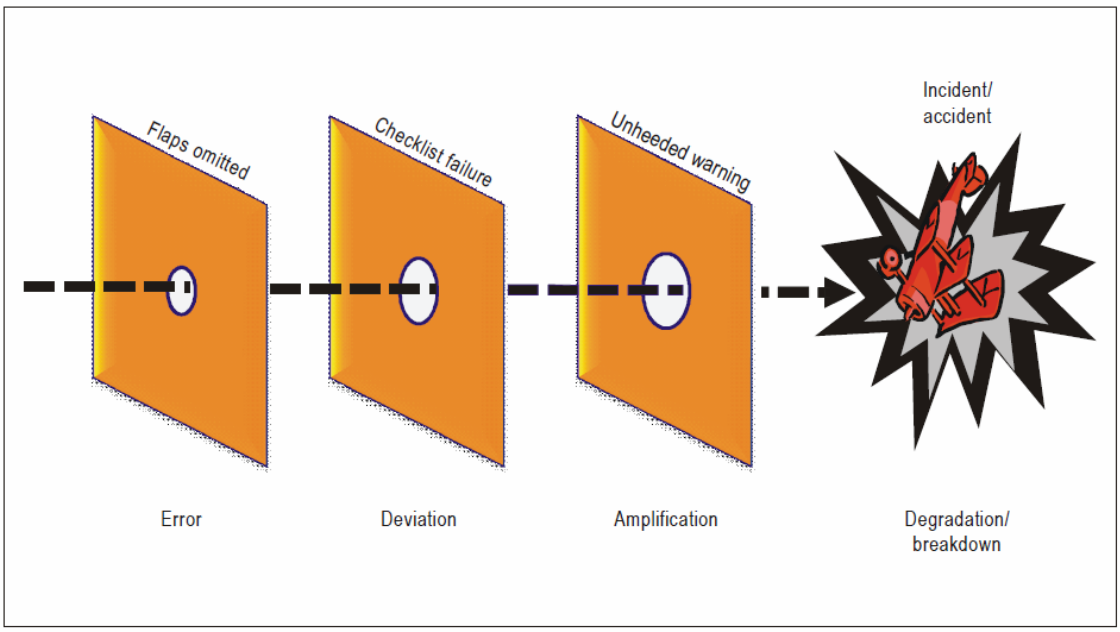
2.7.10 Powszechnym nieporozumieniem jest tworzenie liniowej zależności pomiędzy błędami operacyjnymi a natychmiastowością i znaczeniem ich konsekwencji. To nieporozumienie omówione zostało w punktach 2.6.10 i 2.6.11 w kategoriach błędów operacyjnych i zakresu ich skutków. Dowiedziono, że nie ma symetrii pomiędzy błędami operacyjnymi i zakresem ich potencjalnych konsekwencji. Ponadto zakres konsekwencji błędów operacyjnych jest funkcją raczej kontekstu operacyjnego, w którym zdarzają się, a nie konsekwencji samych błędów. Omówienie to kontynuowane jest poniżej w kategoriach błędów operacyjnych i natychmiastowości ich konsekwencji.

2.7.11 Jest faktem statystycznym, że w lotnictwie dokonuje się codziennie milionów błędów operacyjnych zanim nastąpi poważne obniżenie poziomu bezpieczeństwa (Rysunek 2-10). Pominąwszy nieznaczne fluktuacje pomiędzy latami, dane z ostatniej dekady konsekwentnie podają statystykę wypadków na poziomie niższym niż jeden wypadek ze skutkiem śmiertelnym na milion startów. Ujmując to inaczej, w operacjach komercyjnego przewozu lotniczego na świecie, co milion cykli produkcyjnych popełnia się błąd operacyjny z potencjałem na tyle poważnym, że przełamuje on mechanizmy obronne systemu i generuje poważne obniżenie poziomu bezpieczeństwa. Tak czy inaczej, niedopasowania na liniach styku SHEL generują codziennie dziesiątki tysięcy błędów operacyjnych w trakcie normalnej działalności lotniczej. Jednakże owe błędy wyłapywane są przez wbudowane w system mechanizmy obronne, a ich niszczący potencjał jest ograniczany, zapobiegając negatywnym konsekwencjom. Innymi słowy, na porządku dziennym jest kontrola błędów operacyjnych, dokonywana poprzez skuteczne działanie mechanizmów obronnych systemu lotnictwa.

2.7.12 Oto prosty scenariusz operacyjny wyjaśniający asymetrię pomiędzy błędami operacyjnymi a natychmiastowością ich konsekwencji (Rysunek 2-11A). Po uruchomieniu silnika załoga zapomina o ustawieniu klap w pozycji do startu podczas wykonywania czynności po uruchomieniu silników, przewidzianych w instrukcji użytkowania. Popełniono więc błąd operacyjny, ale nie ma żadnych natychmiastowych konsekwencji. Błąd operacyjny przełamał pierwszą warstwę ochronną (instrukcja, lista czynności załogi po uruchomieniu silnika), ale jego niszczycielski potencjał pozostaje w uśpieniu. Nie ma natychmiastowych konsekwencji, błąd operacyjny po prostu pozostaje w systemie w utajeniu.




**Rysunek 2-10. Błędy operacyjne i bezpieczeństwo – nieliniowy związek.**

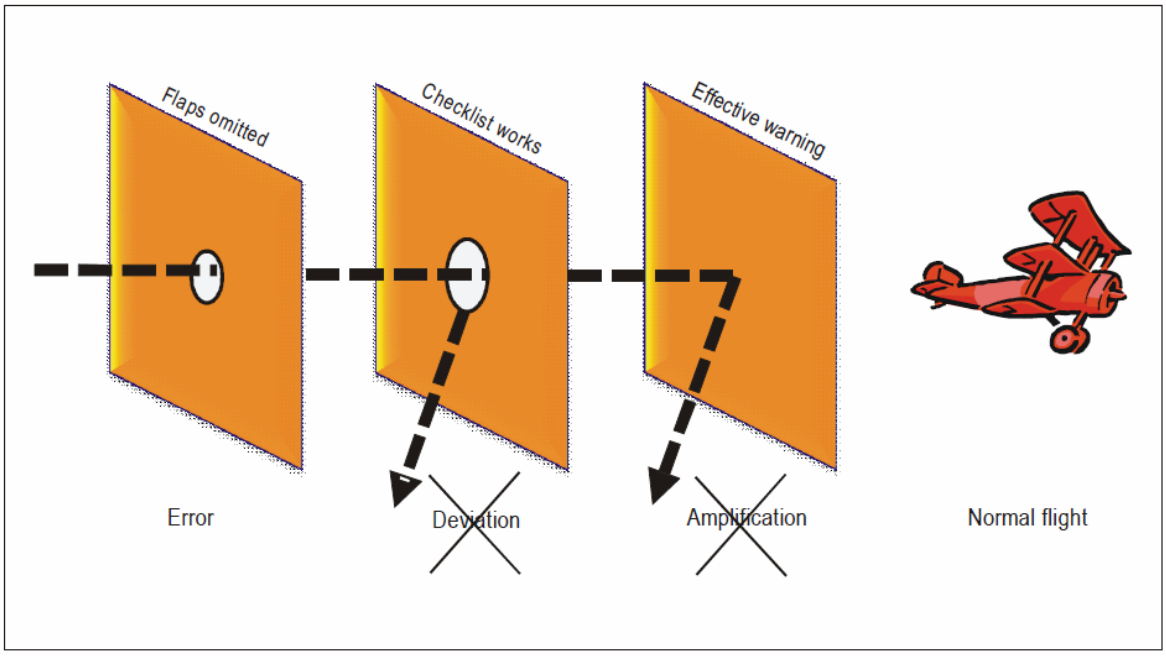



**Rysunek 2-11A. Badanie poważnych awarii — raz na milion lotów**

2.7.13 Załoga wykonuje checklistę po uruchomieniu silników ale nie wykrywa nieprawidłowego położenia klap, a samolot kołuje do startu. Pominięto więc drugą szansę na uniknięcie konsekwencji błędu operacyjnego, który pozostaje w systemie, nadal nieszkodliwy. Niemniej, system jest w stanie odchylenia od normy lub w stanie niepożądanym (tzn. samolot kołujący do startu z nieprawidłowym położeniem klap). Załoga wykonuje checklistę kołowania i przedstartową. W obu przypadkach pomija się nieprawidłowe położenie klap. Kolejne okazje uniknięcia skutków błędu operacyjnego zostają zaprzepaszczone. Błąd operacyjny pozostaje bez konsekwencji, ale status odchylenia od normy lub niepożądany stan systemu pogłębia się.

2.7.14 Załoga rozpoczyna rozbieg, słychać dźwięk ostrzegający o nieprawidłowej konfiguracji do startu. Załoga nie rozpoznaje przyczyny ostrzeżenia i kontynuuje rozbieg. Błąd operacyjny nadal pozostaje bez konsekwencji, ale niepożądany stan systemu pogłębia się. Samolot odrywa się przy nieprawidłowym położeniu klap. System zaczął degradować się, ale załoga nadal może wyprowadzić go ze stanu niepożądanego. Samolot nie może utrzymać się w powietrzu z powodu nieprawidłowego położenia klap i rozbija się. Dopiero w tym momencie, po przełamaniu szeregu wbudowanych w system zabezpieczeń, błąd operacyjny ujawnia swój pełen potencjał niszczący i pociąga za sobą konsekwencje. System doznaje katastroficznego załamania.

2.7.15 Zauważmy stosunkowo znaczny okres pomiędzy popełnieniem błędu operacyjnego przez załogę i nieodwracalnym urzeczywistnieniem się jego niszczycielskiego potencjału. Zauważmy też liczne możliwości uniknięcia konsekwencji błędu operacyjnego dzięki wbudowanym w system zabezpieczeniom. Ten okres to czas, jaki daje system na kontrolę konsekwencji błędów operacyjnych, proporcjonalny do głębokości i wydajności zabezpieczeń systemu. To jest ten okres, w którym można zarządzać bezpieczeństwem przy znacznym prawdopodobieństwie sukcesu.




**Rysunek 2-11B. Zarządzanie bezpieczeństwem – prawie w każdym locie**

2.7.16 Im więcej wbudowanych zabezpieczeń i warstw powstrzymujących zawiera system, tym wydajniejsze jego funkcjonowania i większe możliwości kontroli nad konsekwencjami błędów operacyjnych. Zależność odwrotna jest również prawdziwa.

2.7.17 Z powyższego punktu widzenia oczywistym jest jeden wniosek: scenariusz omówiony w punktach od 2.7.12 do 2.7.14 przedstawia to, co wykryje większość badań wypadków – nieopanowane błędy operacyjne, prowadzące do katastrofalnego załamania systemu. Jest to cenna informacja na temat wad ludzkich i systemowych; informacja ukazująca, co zawiodło, co nie zadziałało, jakie mechanizmy obronne nie funkcjonowały tak jak zakładano. Choć jest ona cenna jako punkt wyjścia, informacja ta nie wystarczy, aby w pełni zrozumieć załamania bezpieczeństwa i powinna być uzupełniona o informacje z innych źródeł.

2.7.18 Rozważmy zmienioną wersję scenariusza omówionego w punktach od 2.7.12 do 2.7.14 (Rysunek 2-11B). Zauważmy, że są przynajmniej cztery oczywiste przypadki, kiedy mechanizmy obronne mogły być uruchomione, aby powstrzymać ujawnienie niszczycielskiego potencjału początkowego błędu operacyjnego (pominięcie ustawienia klap):

a) checklista po uruchomieniu silnika;

b) checklista kołowania;

c) checklista przed startem;

d) ostrzeżenie o nieprawidłowej konfiguracji startowej.

2.7.19 Są również inne przykłady, nie tak oczywiste, jednakże możliwe, kiedy mechanizmy obronne mogły zostać uaktywnione: ostrzeżenie ze strony personelu naziemnego, załóg podobnych samolotów, kontrolerów ruchu lotniczego, etc. Efektywne zadziałanie mechanizmów obronnych w każdym z tych przypadków mogłoby powstrzymać konsekwencje początkowego błędu operacyjnego i przywrócić system do normalnego stanu. Niszczący potencjał błędu operacyjnego można by było wyeliminować w każdym z przypadków, w rezultacie eliminując błąd operacyjny.

2.7.20 Wniosek jest taki, że scenariusze, w których błędy operacyjne wywołują katastrofalne załamania systemu, są rzadkie; zaś scenariusze, w których błędy operacyjne wywołują niepożądane stany systemu (odchylenie, degradacja) występują często. Scenariusze te przedstawiają informację o tym, co początkowo nie zadziałało, ale w głównej mierze o tym, co później działało, w tym o mechanizmach obronnych działających zgodnie z planem. To jest ten typ informacji, który przekazują źródła informacji o bezpieczeństwie alternatywne bądź uzupełniające w stosunku do informacji z badania wypadków. Informacja z badania wypadku z pewnością wskazałaby cztery przypadki, kiedy mechanizmy obronne powinny były być uruchomione, ale najprawdopodobniej może też wskazać tylko dlaczego ich nie uruchomiono.

2.7.21 Te dodatkowe źródła informacji wskazałyby przypadki, kiedy mechanizmy obronne powinny być uruchomione oraz opisałyby jakie one były i jak funkcjonowały. Źródła te opisują sukcesy, więc połączenie informacji z badania wypadków z informacją z tych alternatywnych źródeł tworzy bardziej kompletny obraz konkretnych problemów bezpieczeństwa. Co więcej, ponieważ scenariusze takie jak opisany powyżej, zdarzają się często, alternatywne źródła informacji o bezpieczeństwie, jeśli się do nich sięgnie, mogą dostarczyć znaczną ilość stale napływających informacji, w przeciwieństwie do sporadycznie otrzymywanych informacji z badania wypadków. Pozwoli to na lepsze zrozumienie możliwości wystąpienia załamań systemu. Wniosek, jaki płynie z drugiego scenariusza jest taki, że odporność systemu na zagrożenia nie jest kwestią funkcjonowania wolnego od błędów a efektywnego zarządzania błędami operacyjnymi.

**Trzy strategie kontroli nad błędami operacyjnymi**

2.7.22 Trzy podstawowe strategie kontroli nad błędami operacyjnymi opierają się na trzech podstawowych mechanizmach obronnych systemu lotniczego: technice, szkoleniu i przepisach (w tym procedurach).

2.7.23 ***Strategie redukcji*** działają bezpośrednio na źródło błędu operacyjnego poprzez redukowanie bądź eliminowanie czynników sprzyjających powstaniu błędu. Przykłady strategii redukcji obejmują poprawę dostępu obsługi do różnych elementów statku powietrznego, poprawę oświetlenia przy wykonywaniu czynności, ograniczenie zakłóceń środowiskowych, tzn.:

a) projektowanie skoncentrowane na człowieku;

b) czynniki ergonomiczne;

c) szkolenie.

2.7.24 ***Strategie przechwytywania*** zakładają, że błąd operacyjny został już popełniony. Ich celem jest „przechwycenie” błędu operacyjnego zanim odczuwalne będą jakiekolwiek jego negatywne konsekwencje. Strategie przechwytywania różnią się od strategii redukcji tym, że nie służą bezpośrednio eliminacji błędu, tj.:

a) checklisty;

b) task cards;

c) flight strips.

2.7.25 ***Strategie tolerancji*** odnoszą się do zdolności systemu do przyjęcia błędu operacyjnego bez poważnych konsekwencji. Przykładem środka służącego zwiększeniu tolerancji systemu na błędy operacyjne jest instalacja wielu systemów hydraulicznych lub elektrycznych w celu uzyskania redundancji albo wprowadzenie programu inspekcji strukturalnej, dającego wiele możliwości wykrycia pęknięcia zmęczeniowego zanim osiągnie ono krytyczny rozmiar, innymi słowy:

a) redundancje systemów;

b) inspekcje strukturalne.

2.7.26 Zarządzanie błędami operacyjnymi nie powinno być ograniczone do personelu bezpośrednio wykonującego zadania. Na pracę tego personelu, zgodnie z modelem SHEL, wpływają czynniki organizacyjne, regulacyjne i środowiskowe. Na przykład procesy organizacyjne, takie jak niewystarczająca komunikacja, niejednoznaczne procedury, nierozsądne harmonogramy, niewystarczające zasoby i nierealistyczne budżetowanie tworzą warunki sprzyjające błędom operacyjnym. Jak omówiono wyżej, wszystkie te czynniki są procesami, które organizacja musi w rozsądnym zakresie kontrolować bezpośrednio.

**Błędy a naruszenia**

2.7.27 Jak dotąd w niniejszej części koncentrowaliśmy się na błędach operacyjnych, scharakteryzowanych jako normalne składniki każdego systemu, w którym oddziałują na siebie ludzie i technika, w celu osiągnięcia celów produkcyjnych systemu. Teraz skupimy się na naruszeniach, które są całkiem odmienne od błędów operacyjnych. Jedne i drugie mogą prowadzić do wadliwego działania systemu i mogą doprowadzić do sytuacji o bardzo poważnych konsekwencjach. Jasne rozróżnienie i zrozumienie błędów operacyjnych i naruszeń jest niezbędne do zarządzania bezpieczeństwem.

2.7.28 Istota różnicy pomiędzy błędami operacyjnymi a naruszeniami leży w zamiarze. Podczas gdy błąd jest niezamierzony, naruszenie jest działaniem celowym. Osoby popełniające błędy operacyjne starają się postępować właściwie, ale ze względu na wiele powodów omówionych w poprzednich akapitach poświęconych błędom operacyjnym, nie udaje im się osiągnąć tego, co zamierzają. Z drugiej strony, osoby popełniające naruszenia wiedzą, że ich zachowanie odchodzi od ustalonych procedur, scenariuszy postępowania, norm i praktyk, lecz czynią to rozmyślnie.

2.7.29 Na przykład kontroler zezwala statkowi powietrznemu na zniżanie przez poziom lotu innego statku powietrznego, przy odległości wg DME pomiędzy nimi wynoszącej 18 mil morskich, w sytuacji, w której minimalna separacja powinna wynosić 20 NM. Jeżeli kontroler pomylił się przy obliczaniu różnicy odległości wg DME podawanych przez pilotów, byłby to błąd operacyjny. Jeżeli zaś kontroler prawidłowo obliczył odległość i zezwolił zniżającemu się statkowi powietrznemu na przecięcie poziomu drugiego statku powietrznego, wiedząc, że nie zachowano minimalnej separacji, byłoby to naruszenie.

2.7.30 W lotnictwie większość naruszeń jest wynikiem wadliwych lub nierealistycznych procedur, kiedy pracownicy opracowali sposoby ich obejścia, aby można było w ogóle wykonać zadanie. Większość wynika z autentycznego pragnienia prawidłowego wykonania pracy. Istnieją dwa ogólne typy naruszeń: naruszenia sytuacyjne i rutynowe.

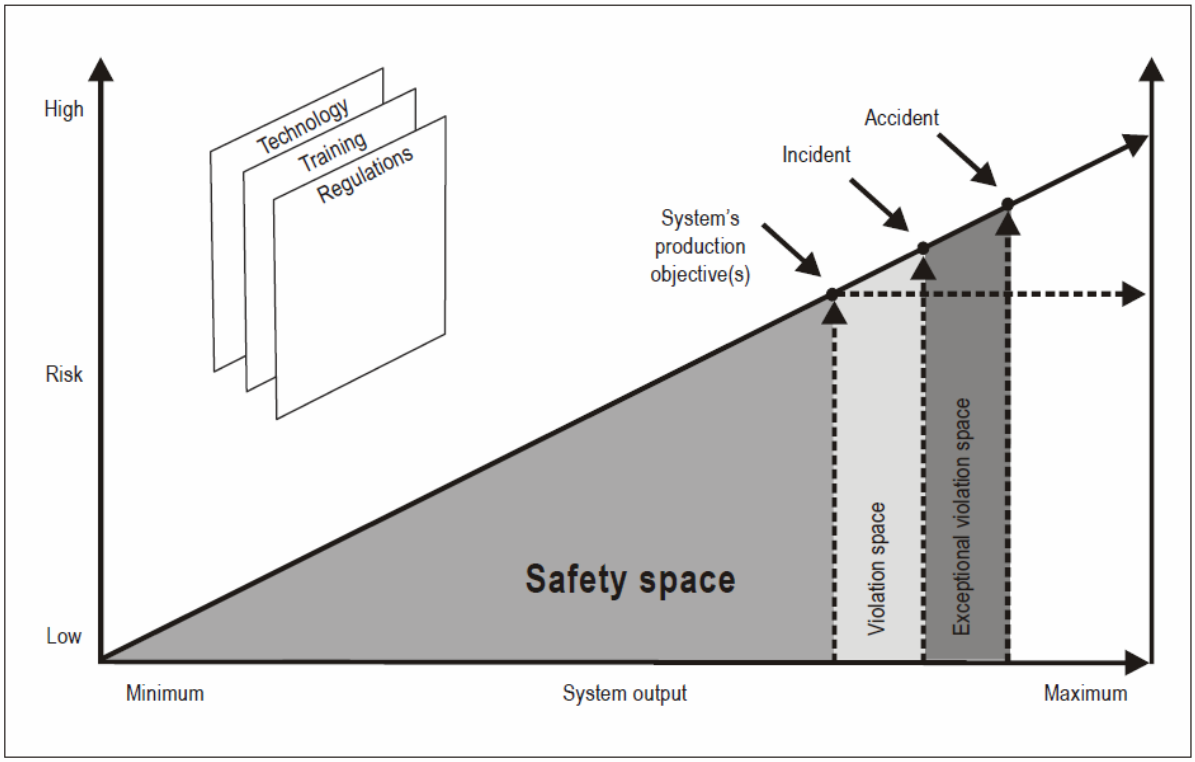
2.7.31 ***Naruszenia sytuacyjne*** zdarzają się z powodu określonych warunków występujących w danym czasie, takich jak presja czasu lub natłok zadań. Pomimo świadomości popełniania naruszenia, przeważa zorientowanie na cel i wypełnienie zadania, co skłania ludzi do odchylenia od normy, w przekonaniu, że odchylenie to nie przyniesie negatywnych konsekwencji.

2.7.32 ***Naruszenia rutynowe*** to naruszenia, które stały się „normalnym sposobem wykonywania pracy" w zespole. Zdarzają się, kiedy zespół ma problem z przestrzeganiem ustalonych procedur przy wykonywaniu zadania, z powodu niepraktyczności/nierealności, źle zaprojektowanej linii styku człowiek-technika, itp. Wtedy zespół nieformalnie wypracowuje i przyjmuje „lepsze" procedury, które w końcu stają się rutyną. Jest to właśnie pojęcie „normalizacji dewiacji" omówione w punkcie 2.5.4. Zespół rzadko postrzega naruszenia rutynowe jako naruszenia, gdyż celem ich jest wykonanie pracy. Uważa się je za „sposoby optymalizacji", ponieważ mają na celu oszczędność czasu i pracy poprzez uproszczenie zadań (nawet jeśli oznacza to „pójście na skróty").

2.7.33 Trzecim, często pomijanym typem naruszeń, są **naruszenia wywołane przez organizację**, które można pojmować jako rozszerzenie naruszeń rutynowych. Potencjalny wpływ tych naruszeń na bezpieczeństwo może być w pełni zrozumiany wyłącznie w kontekście wymagań nałożonych przez organizację w zakresie świadczenia usług, dla których ją powołano. Rysunek 2-12 przedstawia związek pomiędzy dwoma podstawowymi zagadnieniami, które organizacja musi rozważyć i zbilansować przy świadczeniu usług i określaniu jej procesów organizacyjnych: produkt wyjściowy systemu i związane z nim ryzyko bezpieczeństwa.

2.7.34 W każdej organizacji zajmującej się świadczeniem usług, produkt wyjściowy systemu i ryzyko bezpieczeństwa są ze sobą nierozerwalnie związane. Wraz ze wzrostem popytu na produkt wyjściowy systemu (czyli świadczone usługi) ryzyko związane z bezpieczeństwem również rośnie, ze względu na większą skalę działalności. Dlatego też, jak pokazuje rysunek 2-12, minimalny produkt wyjściowy systemu związany jest z najmniejszym ryzykiem, podczas gdy maksymalny produkt związany jest z największym ryzykiem. Operacje przy ciągłym narażeniu na najwyższy stopień ryzyka są niepożądane, nie tylko z punktu widzenia bezpieczeństwa, ale również ze względów finansowych. Dlatego też organizacja równoważy pożądany produkt i tolerowane ryzyko oraz określa produkt wyjściowy systemu na poziomie niższym niż maksymalny, ale skorelowany z tolerowanym poziomem ryzyka dla bezpieczeństwa. W ten sposób organizacja definiuje cele produkcyjne jako funkcję zrównoważenia akceptowalnego produktu z akceptowalnym ryzykiem.

2.7.35 Jedną z fundamentalnych decyzji związanych z procesem określania celów produkcyjnych (uzgodnionych na podstawie bilansowania produktu systemu i ryzyka dla bezpieczeństwa) jest ustanowienie mechanizmów obronnych, koniecznych do ochrony organizacji przed generowanymi w procesie produkcji ryzykami. Jak już wspomniano, trzema podstawowymi mechanizmami obronnymi lotnictwa są: technika, szkolenie i przepisy (w tym procedury). Dlatego też organizacja definiująca cele produkcyjne musi również zdefiniować narzędzia (urządzenia techniczne) konieczne do bezpiecznego i efektywnego świadczenia usług, to, jak promować zachowania wykazywane przez pracowników, aby można było bezpiecznie i wydajnie używać narzędzi (szkolenie), i zestawu norm i procedur określających pracę personelu (przepisy).




**Rysunek 2-12. Zrozumieć naruszenia**

2.7.36 Tak więc produkt końcowy systemu, poziom ryzyka i mechanizmy obronne spotykają się w punkcie definiującym cele produkcyjne organizacji. Opisują one również granice tego, co można określić jako „obszar bezpieczeństwa organizacji". Obszar bezpieczeństwa to strefa, w której mechanizmy obronne stworzone przez organizację gwarantują maksymalną odporność na ryzyko związane z bezpieczeństwem, na które narażona jest organizacja w czasie realizowania celów produkcyjnych.

2.7.37 Źródłem maksymalnej odporności w obszarze bezpieczeństwa jest to, że mechanizmy obronne stworzone przez organizacje są współmierne do zaplanowanego wyjściowego produktu systemu, który z kolei jest współmierny do tolerowanego ryzyka. Innymi słowy zasoby przeznaczone przez organizację na zabezpieczenia są właściwe i współmierne do działań związanych ze świadczeniem usług. Nie oznacza to, że w organizacji nie może zdarzyć się wypadek, gdyż wypadki są przypadkowymi zdarzeniami wynikającymi z szeregu nieprzewidywalnych okoliczności. Oznacza to, że organizacja posiada rozwiązania w zakresie zarządzania bezpieczeństwem gwarantujące akceptowalny poziom kontroli ryzyka podczas świadczenia usług w przewidywalnych okolicznościach. Po prostu organizacja zrobiła, co tylko mogła najlepiej dla bezpieczeństwa.

2.7.38 Biorąc pod uwagę dynamiczną naturę lotnictwa, organizacje lotnicze mogą okazjonalnie doświadczać przejściowego, krótkookresowego wzrostu popytu na produkt końcowy (tj. zintensyfikowane świadczenie usług), na przykład sezonowe wariacje popytu na miejsca w samolotach, szczególne okoliczności takie jak wydarzenia sportowe o światowym zasięgu, itp. Aby obszar bezpieczeństwa pozostał nienaruszony, organizacja powinna zrewidować i poprzesuwać lub zmodyfikować dotychczasową alokację zasobów, i wzmocnić istniejące mechanizmy obronne, aby przeciwstawić się związanemu ze zwiększoną produkcją zwiększonemu poziomowi ryzyka.

2.7.39 Historia lotnictwa, niestety, pokazuje przeciwne przykłady. Zbyt często, jak widać po przypadkach załamania bezpieczeństwa, organizacje lotnicze starają się poradzić sobie z krótkimi okresami zwiększonej produkcji poprzez „naginanie" mechanizmów obronnych, wybieranie nadgodzin zamiast zatrudnienia dodatkowego personelu, co prowadzi do zwiększenia obciążenia pracą i przemęczenia; używanie urządzeń w „bardziej wydajny" sposób zamiast instalowania kolejnych urządzeń; „optymalizowanie" procedur i zasobów bez zmian w instrukcjach operacyjnych i normach, itd.

2.7.40 Rzeczywistym efektem naginania mechanizmów obronnych jest przesunięcie organizacji poza obszar bezpieczeństwa, najpierw w strefę naruszeń, a później w strefę szczególnych naruszeń. Innymi słowy, aby dostarczyć więcej produktu przy tych samych zasobach, personel operacyjny musi odejść od ustalonych procesów poprzez skróty i obejścia usankcjonowane przez organizację. Personel operacyjny nie decyduje o skrótach i obejściach – decyduje o tym organizacja. Kolokwialne wyrażenie „przeciągać strunę" wymownie opisuje sytuację, w której ludzie zmuszeni są do popełniania usankcjonowanych przez organizację naruszeń, aby dostarczyć produktu niewspółmiernego do przeznaczonych na to zasobów.

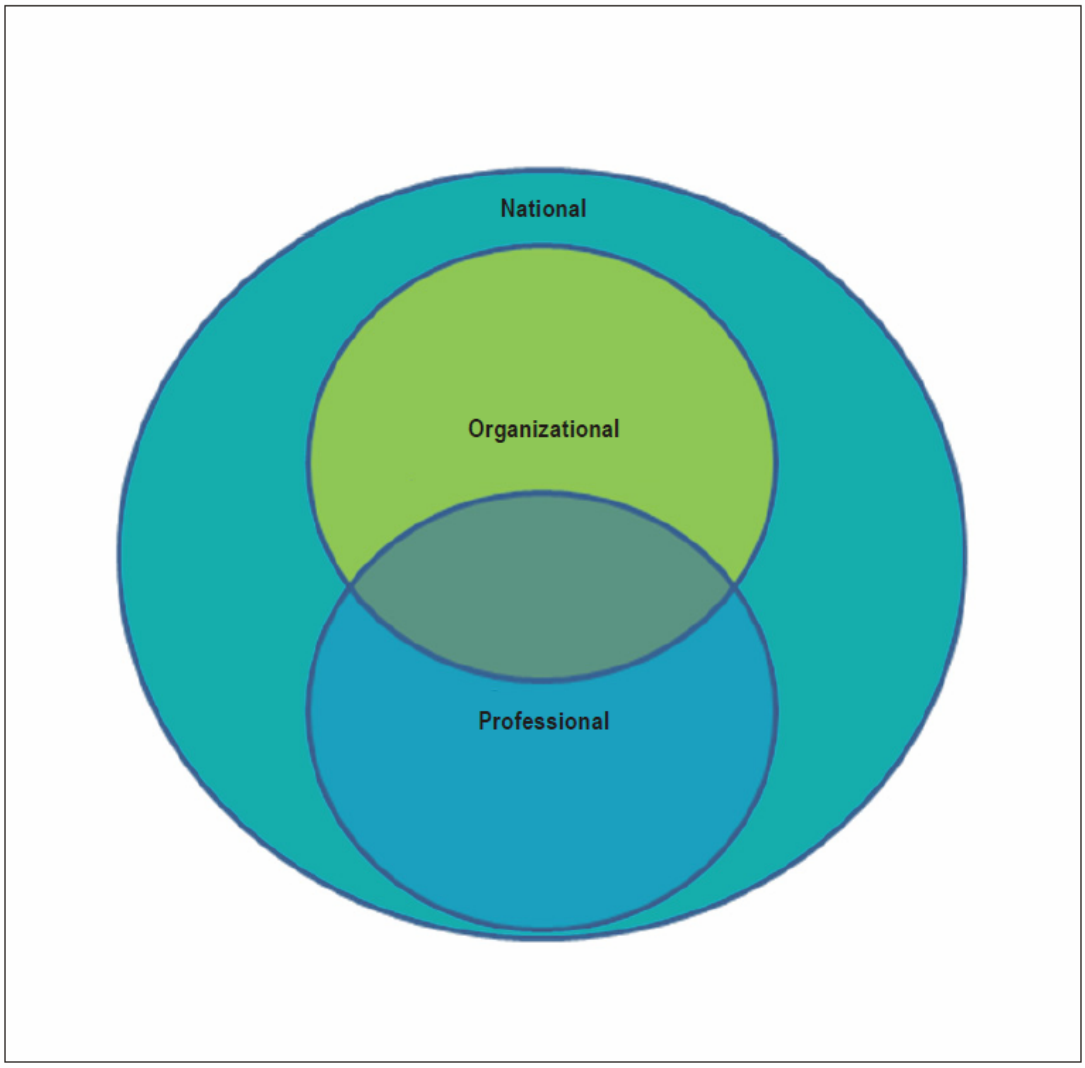
2.7.41 Twardych dowodów na to, że organizacja przesunęła się do strefy naruszeń dostarczają incydenty. Organizacja ucząca się przeanalizuje w takiej sytuacji alokację zasobów, aby poszerzyć swój obszar bezpieczeństwa w celu zachowania harmonii pomiędzy produkcją, tolerowalnym ryzykiem i mechanizmami obronnymi albo, jeśli nie może poszerzyć obszaru bezpieczeństwa, zredukuje produkt wyjściowy systemu. Niektóre organizacje zignorują ostrzeżenia płynące z incydentów, uparcie będą trzymać się dotychczasowych sposobów działania i w nieunikniony sposób przesuną się do strefy wyjątkowych naruszeń. Wypadek stanie się wtedy prawdopodobnym zdarzeniem.

## 2.8. KULTURA ORGANIZACYJNA

2.8.1 Kultura może być opisana w najprostszy sposób, jako "programowanie zbiorowego umysłu". Jeden z najczęstszych opisów graficznych przedstawia kulturę jako "oprogramowanie umysłu". Kultura wpływa na wartości, przekonania i zachowania, które dzielimy z innymi członkami różnych grup społecznych. Kultura łączy nas ze sobą, jako członków grup, dostarcza wskazówek jak zachowywać się w sytuacjach codziennych, a jak w niezwykłych. Kultura określa zasady gry lub ramy we wszystkich kontaktach międzyludzkich. Jest to suma sposobów, w jakich ludzie prowadzą swoje sprawy w określonym środowisku społecznym i stanowi kontekst, w którym coś się dzieje. W odniesieniu do zarządzania bezpieczeństwem, zrozumienie kultury jest równie ważne jak zrozumienie kontekstu, ponieważ kultura jest ważnym wyznacznikiem działań ludzkich.

2.8.2 Badając kulturę, a w szczególności kwestie międzykulturowe, jako że mogą wpływać na bezpieczeństwo lotnicze, łatwo wpaść w pułapkę osądzania, przedstawiając jedną konkretną kulturę, jako możliwie "lepszą" lub" bardziej nadającą się" od innej lub podawanie przykładu danej kultury, jako "złej" lub "nieodpowiedniej" dla konkretnych rozwiązań dotyczących bezpieczeństwa. Jest to nieodpowiednie i bezowocne, ponieważ w badaniu kwestii międzykulturowych ze względu na bezpieczeństwo ważne są różnice, a nie osądzanie. Rzeczywiście istnieją różne kultury i w każdej można odnaleźć istotne zalety i wady. Celem poważnych międzykulturowych badań, w odniesieniu do zarządzania bezpieczeństwem, jest wykorzystanie siły kultury w połączeniu z odpowiednimi praktykami bezpieczeństwa, przy jednoczesnym ograniczeniu negatywnych skutków słabości tych kultur.

2.8.3 Należy mieć świadomość, że kwestie kulturowe wpływają na organizacje, jako że są one zbiorowiskami ludzi. Funkcjonowanie organizacji podlega wpływom kulturowym na każdym poziomie. Poniższe trzy rodzaje kultury (Rysunek 2-13) mają znaczenie dla inicjowania rozwiązań w zarządzaniu bezpieczeństwem, ponieważ warunkują one funkcjonowanie organizacji.




**RYSUNEK 2 – 13. Trzy różne modele kulturowe**

a) **Kultura narodowa** odróżnia cechy narodowe i systemy wartości poszczególnych narodów. Ludzie różnych narodowości różnią się, na przykład, stosunkiem do władzy, radzeniem sobie z niepewnością i niejasnymi sytuacjami, a także sposobem wyrażania swojej indywidualności. Nie wszyscy ludzie są jednakowo dostosowani do zbiorowych potrzeb grupy (zespołu lub organizacji), np. w kulturach kolektywistycznych istnieje akceptacja nierównego statusu i szacunku dla przywódców. Może to mieć wpływ na podważenie decyzji lub działań podejmowanych przez osoby starsze wiekiem, co jest ważnym czynnikiem w pracy grupowej. Zatem, nieporozumienia wynikające z różnorodności kulturowej mogą mieć wpływ na efekty pracy zespołowej.

b) **Kultura zawodowa** rozróżnia cechy i system wartości poszczególnych grup zawodowych (typowe zachowanie pilotów, kontrolerów ruchu lotniczego, inżynierów obsługi). Poprzez dobór pracowników, ich edukację i szkolenie, doświadczenie nabywane w pracy, presję otoczenia, itp., specjaliści (lekarze, prawnicy, piloci, kontrolerzy) przyjmują system wartości, wypracowują zachowania typowe dla danej grupy. Na ogół są oni dumni ze swojego zawodu i chcą być w nim najlepsi. Z drugiej strony, mogą oni przyjąć systemy wartości, które prowadzą do rozwoju poczucia osobistej nietykalności, uczucia, że osobiste problemy nie mają wpływu na wydajność lub że nie popełnią błędów w sytuacjach silnego stresu.

c) **Kultura organizacyjna** odróżnia cechy i systemy wartości poszczególnych organizacji (zachowanie członków jednej firmy w porównaniu do innej lub pracowników rządowych wobec zatrudnionych w sektorze prywatnym) i ma na celu zapewnienie osłony przed wpływem zachowań wynikających z kultur narodowych i zawodowych. Na przykład w liniach lotniczych, piloci mogą pochodzić z różnych środowisk zawodowych (z wojskowym lub cywilnym doświadczeniem, małych lub dużych operatorów). Mogą oni również pochodzić z różnych kultur organizacyjnych powstałych w wyniku fuzji lub zwolnień.

2.8.4 Powyższe trzy rodzaje kultur oddziałują wzajemnie na siebie w kontekście operacyjnym i wpływają między innymi na:

a) relacje pomiędzy młodszymi i starszymi;

b) wymianę informacji;

c) reakcję personelu w trudnych warunkach operacyjnych;

d) sposób wykorzystania rozwiązań technologicznych;

e) reakcje władzy wobec niewłaściwych działań w wyniku błędów operacyjnych (karanie przestępstw czy wnioskowanie z doświadczeń);

f) stosowanie automatyki;

g) rozpowszechnianie procedur (SOP);

h) przygotowanie, przedstawienie i przekazanie dokumentacji;

i) przygotowanie i prowadzenie szkoleń;

j) realizację przydzielonych prac;

k) wzajemnie relacje różnych grup zawodowych (piloci, ATC, personel obsługi, personel pokładowy);

l) współpracę kierownictwa i związków.

Innymi słowy, kultura wpływa praktycznie na każdy typ interpersonalnych i organizacyjnych interakcji. Ponadto względy kulturowe mają odzwierciedlenie w projektowaniu sprzętu i narzędzi. Technologia może wydawać się kulturowo neutralna, jednak odzwierciedla uprzedzenia producenta (np. język angielski stosowany w dużej części świata do programowania komputerowego). Każdy z omówionych powyżej rodzajów kultury posiada mieszankę mocnych i słabych stron.

2.8.5 Największe możliwości tworzenia i skutecznego kreowania kultury zarządzania bezpieczeństwem powstają na poziomie organizacyjnym. System wartości organizacji ma wpływ na zachowanie personelu operacyjnego. Czy organizacja docenia działania w zakresie bezpieczeństwa, wspiera indywidualne inicjatywy, zniechęca lub zachęca do tolerowania ryzyka bezpieczeństwa, egzekwuje ścisłe przestrzeganie SOP, toleruje nieprzestrzeganie SOP lub promuje otwartą dwukierunkową komunikację? W ten sposób organizacja jest głównym wyznacznikiem zachowań pracowników operacyjnych. Kultura organizacyjna określa granice akceptowalnych wyników pracy, poprzez ustanowienie norm i limitów. Tak więc, kultura organizacyjna stanowi podstawę dla kierowniczej kadry i pracowników do podejmowania decyzji.
"Tutaj postępujemy i mówimy w następujący sposób".

2.8.6 Kultura organizacyjna zatem składa się ze wspólnych przekonań, praktyk i postaw. Słowa i działania kierownictwa wyższego szczebla nadają ton efektywnej, kreatywnej kulturze organizacji. Kultura organizacyjna jest to atmosfera stworzona przez kierownictwo wyższego szczebla, które kształtuje postawy pracowników m.in. wobec praktyk bezpieczeństwa. Następujące czynniki wpływają na kulturę organizacyjną:

a) polityka i procedury;

b) praktyki nadzorcze;

c) cele i planowanie bezpieczeństwa;

d) działania w odpowiedzi na niebezpieczne zachowania;

e) szkolenia i motywacja pracowników;

f) zaangażowanie pracowników.

2.8.7 Ostateczna odpowiedzialność za ustanowienie i przestrzeganie dobrych praktyk bezpieczeństwa spoczywa na kierownictwie organizacji – niezależnie od tego, czy są to linie lotnicze, lotnisko, ATS lub AMO. Etos bezpieczeństwa organizacji jest utworzony od samego początku przez stopień, w jakim kierownictwo wyższego szczebla przyjmuje odpowiedzialność za bezpieczeństwo operacji i działania w przypadku pojawiających się problemów dotyczących bezpieczeństwa.

2.8.8 Podejście kierownictwa liniowego do codziennej działalności jest podstawą generatywnej kultury organizacyjnej w zakresie zarządzania bezpieczeństwem. Czy wyciągane są poprawne wnioski na podstawie rzeczywistych doświadczeń liniowego kierownictwa i czy podejmowane są właściwe działania? Czy pracownicy, których dane zdarzenie dotyczy są konstruktywnie zaangażowani w proces naprawczy, czy też czują, że są ofiarami jednostronnych działań podejmowanych przez zarządzających?

2.8.9 Stosunki kierownictwa liniowego z przedstawicielami władz wpływają także na generatywną kulturę organizacyjną. Stosunki te powinny się charakteryzować profesjonalną uprzejmością, ale przy zachowaniu odpowiedniego dystansu, tak aby nie wpływać niekorzystnie na kwestie odpowiedzialności. Otwartość przyczynia się do lepszego komunikowania o bezpieczeństwie niż ścisłe egzekwowanie przepisów. To pierwsze zachęca do konstruktywnego dialogu, podczas gdy to drugie przyczynia się do ukrywania lub ignorowania rzeczywistych problemów bezpieczeństwa.

2.8.10 Chociaż zgodność z przepisami bezpieczeństwa ma kluczowe znaczenie dla rozwoju dobrych praktyk bezpieczeństwa, współcześnie uważa się, że konieczne jest znacznie więcej. Organizacje, które po prostu są zgodne z minimalnymi standardami określonymi przez przepisy nie są w dobrej pozycji, by identyfikować problemy związane z bezpieczeństwem.

2.8.11 Efektywnym sposobem promowania bezpieczeństwa operacji lotniczych jest zapewnienie, że operator wypracował w obszarze operacyjnym warunki, gdzie wszyscy pracownicy czują się odpowiedzialni za bezpieczeństwo i zastanawiają się w jaki sposób to, co robią wpływa na bezpieczeństwo. Ten sposób myślenia musi być tak głęboko zakorzeniony w ich działalność, aby był rozumiany jako "nasz sposób prowadzenia działalności". Wszystkie podejmowane decyzje, czy to przez zarząd, kierowcę na płycie lotniska, czy też przez inżyniera, należy rozważyć pod kątem wpływu na bezpieczeństwo.

2.8.12 Takie środowisko operacyjne musi funkcjonować zgodnie z zasadą "z góry na dół" (top-down management) i opiera się na wysokim stopniu zaufania, i szacunku między pracownikami a kierownictwem. Pracownicy muszą wierzyć, że będą wspierani w każdej decyzji podjętej w interesie bezpieczeństwa. Muszą również zrozumieć, że umyślne naruszenia i działania zagrażające bezpieczeństwu nie będą tolerowane.

**Efektywne raportowanie bezpieczeństwa**

2.8.13 Jednym z najbardziej znaczących aspektów kultury organizacyjnej w zakresie zarządzania bezpieczeństwem jest struktura raportowania o bezpieczeństwie oraz procedury i praktyki personelu. Identyfikacja zagrożeń jest podstawą w zarządzania bezpieczeństwem. Najodpowiedniejszymi osobami do zgłaszania zagrożeń, tego co funkcjonuje tak, jak powinno, a co nie, są pracownicy operacyjni, którzy spotykają się z zagrożeniami na co dzień. Efektywne raportowanie zagrożeń bezpieczeństwa przez personel operacyjny jest zatem podstawą zarządzania bezpieczeństwem. Dlatego obszar operacyjny, w którym personel operacyjny został wyszkolony i jest nieustannie zachęcany do zgłaszania zagrożeń jest warunkiem skutecznego raportowania bezpieczeństwa.

2.8.14 Efektywne raportowanie bezpieczeństwa opiera się na następujących podstawowych cechach:

a) zarząd kładzie bardzo silny nacisk na identyfikację zagrożeń w ramach strategii zarządzania bezpieczeństwem, co w konsekwencji wpływa na świadomość znaczenia komunikowania informacji o zagrożeniach na wszystkich poziomach organizacji;

b) kierownictwo wyższego szczebla i personel operacyjny mają realistyczne spojrzenie na zagrożenia w działalności organizacji, w konsekwencji czego istnieją realistyczne zasady działania odnoszące się do zagrożeń i potencjalnych źródeł szkód;

c) kierownictwo wyższego szczebla określa wymogi operacyjne, niezbędne do wspierania aktywnego raportowania zagrożeń, zapewnia, że kluczowe dane dotyczące bezpieczeństwa są prawidłowo zarejestrowane, demonstruje otwarte podejście do zgłaszania zagrożeń przez personel operacyjny i wdraża środki w celu wyeliminowania skutków zagrożeń;

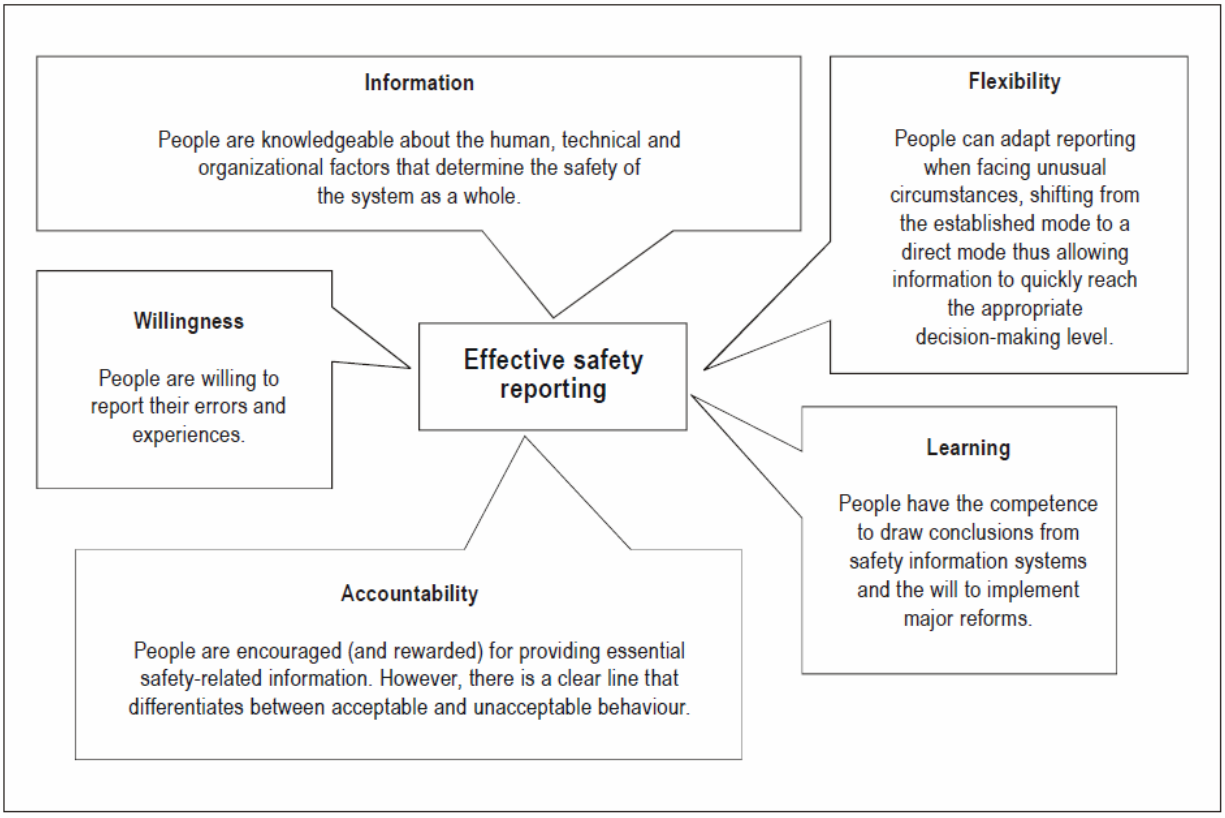
d) kierownictwo wyższego szczebla zapewnia, że kluczowe dane dotyczące bezpieczeństwa są należycie zabezpieczone i promuje system kontroli, zgodnie z którym raportujący o zagrożeniach są pewni, że zawiadomienie o zagrożeniu nie będzie wykorzystane do innego celu niż ten, dla którego zostało złożone (zarządzanie bezpieczeństwem);

e) personel jest wyszkolony do rozpoznawania i zgłaszania zagrożeń oraz rozumie naturę i konsekwencje zagrożeń w działaniach organizacji;

f) niebezpieczne zachowania występują z małą częstotliwością, a etyka bezpieczeństwa zniechęca do takich zachowań.

**Efektywne raportowanie bezpieczeństwa – Pięć podstawowych cech**

2.8.15 Istnieje pięć podstawowych cech, które są powszechnie związane z systemami efektywnego raportowania o bezpieczeństwie (Rysunek 2-14). Są one związane z podstawowymi atrybutami skutecznego raportowania, które zostały omówione w punkcie 2.8.14.




**Rysunek 2-14. Skuteczne zawiadamianie o zagrożeniach – Pięć podstawowych elementów**

a) ***Chęć.*** W wyniku przemyślanych działań kierownictwa wyższego szczebla, mających na celu określenie wymogów operacyjnych, niezbędnych dla wspierania aktywnej sprawozdawczości o zagrożeniach oraz zapewnienie, że kluczowe dane dotyczące bezpieczeństwa są prawidłowo zarejestrowane, personel operacyjny chętnie zgłasza zagrożenia i ewentualne błędy operacyjne, które mogą wynikać z istnienia zagrożeń lub osobistych doświadczeń personelu.

b) ***Informacja.*** W następstwie formalnych szkoleń dotyczących rozpoznawania i zawiadamiania o zagrożeniach, a także o naturze i konsekwencjach zagrożeń w działaniach organizacji, personel operacyjny posiada wiedzę o czynniku ludzkim, technicznym i organizacyjnym, które determinują bezpieczeństwo systemu jako całości.

c) ***Elastyczność***. Posiadając realną wiedzę o podstawowych zagrożeniach w działalności organizacji i zasadach odnoszących się do zagrożeń oraz potencjalnych źródeł zniszczeń, personel operacyjny może dostosować raportowanie zagrożeń do okoliczności; kiedy to potrzebne, odchodząc od ustalonego trybu działania, umożliwiając w ten sposób przekazanie informacji do odpowiednich poziomów decyzyjnych.

d) ***Edukacja.*** Mając świadomość znaczenia zawiadamiania o zagrożeniach na wszystkich poziomach działalności organizacji, personel operacyjny czuje się kompetentny do wyciągania wniosków z systemów informacji o bezpieczeństwie, przy jednoczesnej woli organizacji do wprowadzania kluczowych reform.

e) ***Odpowiedzialność.*** W konsekwencji tego, że kluczowe dane dotyczące bezpieczeństwa są prawidłowo zabezpieczone, a system kontroli zapewnia, że raportujący o zagrożeniach są pewni, że ich zawiadomienia nie zostaną wykorzystane do innych celów niż te, w jakich zostały złożone, personel operacyjny czuje się zachęcany do przekazywania niezbędnych informacji dotyczących bezpieczeństwa (i jest za takie postępowanie nagradzany). Dopuszczalne i niedopuszczalne zachowania są jednak wyraźnie rozróżnione.

2.8.16 Efektywne raportowanie bezpieczeństwa jest podstawą zarządzania bezpieczeństwem. Po zgłoszeniu, dane na temat zagrożeń stają się informacjami dotyczącymi bezpieczeństwa. Efektywne raportowanie bezpieczeństwa jest więc podstawą zbierania danych dotyczących bezpieczeństwa. Po otrzymaniu danych dotyczących bezpieczeństwa muszą one podlegać procesowi zarządzania. Zarządzanie danymi o bezpieczeństwie opiera się na trzech wyraźnych krokach. Pierwsze dwa kroki dotyczą zbierania danych bezpieczeństwa oraz ich analizy, w wyniku której przekształcane są w informacje dotyczące bezpieczeństwa. Trzecim, często pomijanym krokiem, jest podjęcie działań w związku z informacjami dotyczącymi bezpieczeństwa. Organizacja może odpowiedzieć na informacje o zagrożeniach w bezpieczeństwie w różny sposób, od zmniejszania zagrożenia do jawnego lekceważenia.

2.8.17 Literatura charakteryzuje trzy rodzaje organizacji w zależności od tego jak odpowiadają na informacje o zagrożeniach i jak nimi zarządzają:

a) patologiczna – ukrywa informacje;

b) biurokratyczna – ogranicza dostęp do informacji;

c) generatywna – szanuje informacje.

2.8.18 Tabela 2-1 przedstawia matrycę kluczowych aspektów zarządzania informacjami w zakresie bezpieczeństwa przez trzy rodzaje organizacji omówione w punkcie 2.8.17.

| | *Poor* | *Bureaucratic* | *Positive* |
|---|---|---|---|
| Information | Hidden | Ignored | Sought |
| Messengers | Shouted | Tolerated | Trained |
| Responsibilities | Shirked | Boxed | Shared |
| Reports | Discouraged | Allowed | Rewarded |
| Failures | Covered up | Merciful | Scrutinized |
| New ideas | Crushed | Problematic | Welcomed |
| Resulting organization | Conflicted organization | Red tape organization | Reliable organization |
| *Source: Ron Westrum* | | | |

**Tabela 2-1. Trzy możliwe modele kultur organizacyjnych**

**Efektywne zawiadamianie i kultura bezpieczeństwa**

2.8.19 Dobrowolne systemy raportowania, które po raz pierwszy opracowano pod koniec lat 70-tych koncentrowały się na zgłaszaniu błędów operacyjnych, wynikających z istniejących warunków i okoliczności. Skuteczne raportowanie bezpieczeństwa, jak opisuje ten podręcznik, sięga dalej. Uważa się, że należy wyszukiwać i określać przyczyny błędów operacyjnych, tak aby mogły one zostać usunięte lub złagodzone zanim pojawi się zagrożenie. Doprowadziło to do powstania systemów dobrowolnego zgłaszania, które obejmują także zgłaszanie zagrożeń. Przyjęto generalną zasadę, że należy zarządzać zagrożeniami i że zapewnienie bezpieczeństwa operacji jest bardziej praktyczne, łatwiejsze i, w dużym stopniu, bardziej skuteczne niż zapewnienie bezpieczeństwa ludzi. Takie podejście jest korzystniejsze dla zarządzania bezpieczeństwem niż tylko raportowanie błędów. Jednakże różnica między raportowaniem błędów a raportowaniem zagrożeń jest zasadnicza i może prowadzić do problemów z wdrażaniem działań, które jednak należy rozpoznać i rozwiązywać. Istotną różnicą jest to, że podczas gdy zgłaszanie zagrożeń jest przewidywalne i powinno być metodą obiektywną i neutralną, to raportowanie błędów jest reaktywne i może obciążać zgłaszającego, co z kolei może prowadzić do wskazywania winy i wymierzania kary.

2.8.20 Efektywne raportowanie bezpieczeństwa opiera się na dobrowolnym raportowaniu o błędach i zagrożeniach. Raportujący to głównie personel operacyjny, który narażony jest na zagrożenia. Jednak ze względu na to, że zagrożenia mogą być także bardziej oczywiste dla osoby z zewnątrz, nie powinno być żadnych ograniczeń co do tego kto i o czym może zawiadamiać. Raportowanie nie powinno być ograniczane w jakikolwiek sposób, a ochrona osób raportujących i źródeł informacji na temat bezpieczeństwa była i jest często kluczową kwestią sporną w tworzeniu obu rodzajów systemów raportowania i może być znaczącą przeszkodą dla rozwoju i sukcesu zarządzania bezpieczeństwem.

2.8.21 Starania o ochronę informacji dotyczących bezpieczeństwa oraz o ochronę przed wymierzaniem kary raportującym o bezpieczeństwie są rozpowszechniane przy użyciu terminów „kultura niekaralności", „kultura nieobwiniania", a ostatnio „kultura bezpieczeństwa" lub „kultura sprawiedliwości". Słowo „kultura" nie ma specyficznego znaczenia, a kontekst, w którym jest stosowane w tym przypadku może prowadzić do błędnego odbioru i nieporozumień. Niemniej jednak bezpieczeństwo i kultura sprawiedliwości stały się szeroko akceptowanymi, choć nie powszechnie zdefiniowanymi, terminami służącymi opisaniu kontekstu okoliczności, na jakich opiera się promowanie bezpieczeństwa w ramach organizacji. Takie praktyki bezpieczeństwa obejmują szereg procesów organizacyjnych, procedur i polityk, które dążą do osiągnięcia konkretnego wyniku, tj. identyfikacji zagrożeń. Procesy (np. efektywne raportowanie bezpieczeństwa), procedury (np. system raportowania zagrożeń) i polityka (np. polityka bezpieczeństwa, sprawiedliwego traktowania raportujących, itp.) są to złożone, konkretne pomysły i zachowania, które mogą być podawane w taki sposób, aby były zrozumiałe dla szerokiej publiczności, a zatem łatwiejsze do zastosowania na dużą skalę. Niemniej jednak, ich istota i zasady stosowania będą odzwierciedlać kulturę, w prawdziwym tego słowa znaczeniu, państwa lub organizacji, w której powstały. Globalne przyjęcie jednej, wspólnej kultury bezpieczeństwa lub sprawiedliwości może zatem zostać uznane za dyskryminujące, jeśli lokalna kultura nie jest taka sama.

2.8.22 Polityka bezpieczeństwa powinna aktywnie promować efektywne raportowanie dot. bezpieczeństwa i poprzez określenie akceptowalnych (często niezamierzone błędy) i nieakceptowalnych zachowań (takich jak niedbalstwo, lekkomyślność, naruszenia lub sabotaż) zapewnić uczciwą ochronę raportujących. Kultura bezpieczeństwa lub sprawiedliwości nie może jednak wykluczać karania za błędy, które z prawnego, etycznego i moralnego punktu widzenia jest zgodne z zasadami funkcjonowania państwa prawa, pod warunkiem, że takie postępowanie jest zgodne z międzynarodowymi ustaleniami. Należy spodziewać się postępowania sądowego i wyciągnięcia jakiejś formy konsekwencji po wypadku lub poważnym incydencie, szczególnie, gdy zginęli ludzie lub uszkodzeniu uległo mienie, nawet jeżeli nie miało miejsca zaniedbanie i nie istniały złe intencje. Potencjalny problem może zatem zaistnieć, jeśli zgłoszenia w dobrowolnym systemie zgłaszania zagrożeń, które odnoszą się do ukrytych braków systemu lub jego działania, są traktowane w ten sam sposób, jak te dotyczące badań wypadków i poważnych incydentów. Ochrona zawiadomień o zagrożeniu nie powinna powodować kwestionowania zasadności dochodzenia sądowego ani prowadzić do nadmiernej nietykalności. Jednak zwykle to argument prawny jest nadrzędnym przed technicznym lub innym związanym z bezpieczeństwem.

2.8.23 Państwa i organizacje powinny wziąć pod uwagę zalety i wady przyjętego systemu kultury bezpieczeństwa i sprawiedliwości, a także wszelkich jej kulturowych i prawnych konsekwencji. Dla celów związanych z zarządzaniem bezpieczeństwem, procesem, który wymaga promowania, pielęgnowania i skutecznej ochrony jest raportowanie o bezpieczeństwie; karanie za błędy ma mniejsze znaczenie. Efektywne raportowanie bezpieczeństwa można osiągnąć na wiele różnych sposobów i za pomocą wielu różnych strategii. Sposób jego osiągnięcia powinien zależeć od preferencji, możliwości i ograniczeń określonego kontekstu operacyjnego, a nie być wynikiem wprowadzania gotowych rozwiązań, które mogłyby kolidować z lokalną kulturą.

## 2.9 BADANIE BEZPIECZEŃSTWA

2.9.1 Badanie zdarzeń jest ważnym elementem zarządzania bezpieczeństwem. Rozdział 7 charakteryzuje proces badania wypadków jako ostateczną obronę w systemie bezpieczeństwa. Wartość badania zdarzeń jest jednak proporcjonalna do podejścia, z jakim prowadzone jest badanie przyczyn zdarzenia.

2.9.2 Tradycyjne podejście omówione w punkcie 2.3.8 opisuje to, co jest znane jako badanie po fakcie:

a) ustalenie strat;

b) umocnienie zaufania i wiary w system;

c) wznowienie normalnej działalności;

d) realizacja celów polityki.

2.9.3 Pojęcie uwarunkowania zdarzenia opisane w pkt. 2.4 i pojęcie wypadku z przyczyn organizacji omówione w pkt. 2.5 są związane z pojęciem badania bezpieczeństwa w celu zwiększenia niezawodności systemu:

a) aby dowiedzieć się o podatności systemu;

b) do opracowania strategii zmian;

c) do priorytetowego traktowania inwestycji w zasoby bezpieczeństwa.

2.9.4 Na zakończenie tego rozdziału przedstawiono schematycznie jeden przykład każdego podejścia do badania bezpieczeństwa. Oba przykłady dotyczą dochodzenia w sprawach wypadków.

### Badanie bezpieczeństwa po fakcie

2.9.5 ***Fakty***

- Czterosilnikowy turbośmigłowy frachtowiec starej generacji w locie krajowym w załodze dwuosobowej leci w warunkach oblodzenia, w nocy.
- W wyniku oblodzenia na silnikach nr 2 i 3 następuje zerwanie płomienia (flameout), a siedem minut później silnik nr 4 przestaje działać. Załoga uruchamia silnik nr 2.
- Statek powietrzny znalazł się w asymetrycznym układzie napędowym z 2 silnikami na lewej stronie dostarczającymi mocy i dwoma po prawej stronie niesprawnymi. Załoga napotyka poważne trudności w kontrolowaniu statku powietrznego.
- Ze względu na duże zapotrzebowanie statku powietrznego na energię pozostałe źródła zasilania nie zapewniają właściwej pracy urządzeń zasilanych energią elektryczną i system zaczyna korzystać z zasilania z akumulatora. Załoga próbuje utrzymać kontrolę nad statkiem powietrznym korzystając z przyrządów w trybie awaryjnym, ograniczając łączność radiową i przy ograniczonych możliwościach nawigowania.
- Podczas próby przeprowadzenia lądowania awaryjnego akumulator jest wyczerpany i brak jest energii elektrycznej.
- Załoga może więc wykorzystywać jedynie przyrządy żyroskopowe z własnym zasilaniem, latarki i przyrządy kontroli pracy sprawnego silnika.
- Załoga nie jest w stanie kontrolować przebiegu lotu i statek powietrzny rozbija się.

2.9.6 ***Wyniki dochodzenia w sprawie badania bezpieczeństwa***

- Załoga nie używała radarów meteorologicznych w celu uniknięcia warunków oblodzenia.
- Załoga nie konsultowała wykazu awaryjnego w celu rozwiązania awarii systemu napędowego i elektrycznego.

- Załoga miała do czynienia z sytuacją, która wymagała szybkiego podjęcia decyzji i zdecydowanego działania.
- Statek powietrzny został oblatany w warunkach oblodzenia, które przekroczyły warunki certyfikacji silników.
- Załoga nie zażądała przekierowania do bliższego lotniska.
- Załoga nie użyła poprawnej frazeologii, aby zakomunikować sytuację awaryjną.
- Załoga praktykowała złe zarządzanie zasobami załogi (CRM).
- Systemy statku powietrznego były źle zarządzane.
- Informacje na liście kontrolnej były źle przedstawione w formie wizualnej.
- Istniały problemy z wewnętrznymi procedurami zapewnienia jakości operacji lotniczych.

2.9.7 ***Przyczyny***

- Różne błędy silnika.
- Niewłaściwie wykonywane ćwiczenia ratownicze.
- Działania załogi lotniczej w celu zabezpieczenia i ponownego uruchamiania silników.
- Opór aerodynamiczny wynikający ze złego ustawienia śmigła (Drag from unfeathered propellers).
- Waga lodu.
- Słaby CRM.
- Brak planów awaryjnych.
- Utrata świadomości sytuacyjnej.

2.9.8 ***Zalecenia dotyczące bezpieczeństwa***

- Władze powinny przypominać pilotom o stosowaniu odpowiedniej frazeologii.
- Władze powinny zastosować jak najbardziej efektywne formy rozpowszechnienia materiału dotyczącego opisanej sytuacji.

**Dochodzenie w sprawie bezpieczeństwa w celu zwiększenia niezawodności systemu**

2.9.9 ***Fakty***

- Dwusilnikowy statek powietrzny turbośmigłowy starszej generacji prowadzący regularny przewóz pasażerski realizuje nieprecyzyjne podejście w marginalnych warunkach pogodowych na lotnisku niekontrolowanym, bez wyposażenia radarowego.
- Załoga przeprowadza podejście do lądowania z prostej, zamiast wykorzystać opublikowaną procedurę podejścia.
- Po osiągnięciu MDA załoga nie osiąga kontaktu wizualnego z ziemią.
- Nie uzyskawszy wizualnego kontaktu z ziemią załoga pomija MDA i podejmuje decyzję o lądowaniu
- W konsekwencji samolot rozbija się po wypadnięciu z pasa startowego.

2.9.10 ***Wyniki dochodzenia w sprawie badania bezpieczeństwa***

- Załoga popełniła wiele błędów i naruszeń.

**Ale:**

- Skład załogi, jakkolwiek właściwy, był niekorzystny ze względu na wymagania dla danego lotu.
- Zgodnie z praktyką firmy, załoga realizuje podejście z prostej, co jest niezgodne z przepisami.
- Państwo nie ustanowiło standardów dla operacji realizowanych mniejszymi statkami powietrznymi,
- Brak nadzoru przez państwo nad obiektami wykorzystywanymi w ruchu lotniczym.
- Władze zlekceważyły wcześniejsze naruszenia bezpieczeństwa przez operatora.
- Przepisy były nieaktualne.
- Władza ustanowiła sprzeczne cele pomiędzy ułatwieniem rozwoju przemysłu a wymaganiami nadzoru.
- Władza nie posiadała właściwych środków do realizacji swoich kompetencji.
- Brak polityki państwa w lotnictwie wspierającej władze lotnicze.
- Braki w państwowym systemie szkolenia.

2.9.11 ***Przyczyny***

- Decyzja załogi o kontynuowaniu podejścia poniżej MDA bez kontaktu wzrokowego z ziemią.
- Na decyzję załogi miała wpływ presja organizacji.
- Na decyzję miał wpływ słaby poziom kultury bezpieczeństwa w linii lotniczej.

2.9.12 ***Zalecenia dotyczące bezpieczeństwa***

- Raport zawiera wiele ważnych zaleceń dotyczących zachowania załogi.
- Raport zawiera również zalecenia w odniesieniu do:
  - Przeglądu procesu udzielania AOC przez władze;
  - Przeglądu systemu szkolenia w państwie;
  - Zdefiniowania polityki w zakresie lotnictwa, która zapewniłaby wsparcie dla zadań realizowanych przez administrację lotniczą;
  - Konieczności nowelizacji obowiązujących przepisów lotniczych;
  - W odniesieniu do zastosowania tymczasowych środków legislacyjnych;
  - Poprawę procesów kontroli statków powietrznych i linii lotniczych oraz badania przyczyn wypadków.

# Rozdział 3

# WPROWADZENIE DO ZARZĄDZANIA BEZPIECZEŃSTWEM

## 3.1 CEL I ZAWARTOŚĆ

3.1. 1 W tym rozdziale omówiona zostanie potrzeba, strategie i kluczowe aspekty zarządzania bezpieczeństwem. Niniejszy rozdział podejmuje kwestie różnic pomiędzy zarządzaniem bezpieczeństwem jako procesem organizacyjnym oraz zapobieganiem wypadkom jako czynności zaradczej.

3.1. 2 Rozdział zawiera następujące tematy:

a) Stereotyp dotyczący bezpieczeństwa;

b) Dylemat zarządzania;

c) Potrzeba zarządzania bezpieczeństwem;

d) Strategie zarządzania bezpieczeństwem;

e) Konieczność zmiany;

f) Zarządzanie bezpieczeństwem – osiem części składowych;

g) Cztery obowiązki w zarządzaniu bezpieczeństwem.

## 3.2 STEREOTYP DOTYCZĄCY BEZPIECZEŃSTWA

3.2.1 W lotnictwie panuje wszechobecne, błędne postrzeganie kwestii tego, na którym miejscu powinno stawiać się bezpieczeństwo w całym spektrum celów, do których dążą organizacje lotnicze, bez względu na naturę usług, jakie te organizacje mogą świadczyć.

3.2.2 Wszystkie organizacje lotnicze, bez względu na ich naturę, mają zawarty element biznesowy, w większym lub mniejszym stopniu. Stąd wszystkie mogą być postrzegane jako organizacje o charakterze biznesowym. Zatem istotne jest zadanie prostego pytania, które naświetli kwestie prawdziwości lub jej braku w sprawie stereotypu bezpieczeństwa: co jest fundamentalnym celem organizacji biznesowej? Odpowiedź na to pytanie jest oczywista: po pierwsze świadczenie usług, dla których organizacja została powołana, aby osiągnąć cele produkcyjne, a w końcu przekazanie dywidendy udziałowcom.

3.2.3 Nie ma żadnej organizacji lotniczej, która została powołana by zajmować się tylko bezpieczeństwem. Nawet organizacje, które funkcjonują jako „strażnicy” bezpieczeństwa lotniczego są podmiotem wewnętrznych lub zewnętrznych ograniczeń wydajności, wyznaczanej przez ich udziałowców. To dotyczy również Międzynarodowej Organizacja Międzynarodowego Lotnictwa Cywilnego, narodowych i ponadnarodowych władz lotnictwa cywilnego, międzynarodowych organizacji handlowych oraz międzynarodowych organizacji na rzecz bezpieczeństwa.

3.2.4 W rozdziale drugim omówione zostało bezpieczeństwo widziane coraz częściej jako konsekwencja zarządzania pewnym procesem organizacyjnym, z ostatecznym celem utrzymania ryzyka jako konsekwencji zagrożeń w kontekście operacyjnym w ramach kontroli organizacyjnej. Zarządzanie określonym procesem organizacyjnym, przede wszystkim związanym z biznesem, jest niezbędnym warunkiem umożliwiającym organizacjom osiągnięcie założonych przez nie celów produkcyjnych poprzez świadczenie usług. Te procesy organizacyjne, takie jak: komunikacja, przydzielanie środków, planowanie i nadzór, również były omawiane w rozdziale drugim. Zarządzanie tymi procesami jest dokonywane poprzez podstawowe funkcje biznesowe i systemy zarządzania, takie jak zarządzanie finansami, zasobami ludzkimi oraz kontrola prawna.

3.2.5 Perspektywa rozwinięta w tym podręczniku zakłada, że bezpieczeństwo nie jest priorytetem organizacji lotniczych. Raczej, zarządzanie bezpieczeństwem jest właśnie jeszcze jednym procesem organizacyjnym, który pozwala organizacjom lotniczym osiągnąć ich biznesowe założenia poprzez świadczenie usług. Dlatego zarządzanie bezpieczeństwem jest właśnie kolejną, podstawową funkcją biznesu, która musi być brana pod uwagę w tym samym stopniu i z tą samą wagą jak inne podstawowe funkcje biznesowe i jest ono realizowane poprzez określony system zarządzania (system zarządzania bezpieczeństwem lub SMS, omawiany w rozdziale 7).

### 3.3 DYLEMAT ZARZĄDZANIA

3.3.1 Pogląd o uznaniu zarządzania bezpieczeństwem za proces organizacyjny oraz za podstawową funkcję biznesową jasno stawia najwyższą odpowiedzialność za tę funkcję na najwyższych szczeblach organizacji lotniczych (nie odbierając znaczenia indywidualnej odpowiedzialności za bezpieczeństwo przy świadczeniu usług). Taka odpowiedzialność nigdzie nie jest bardziej widoczna niż w decyzjach dotyczących przydzielania zasobów.

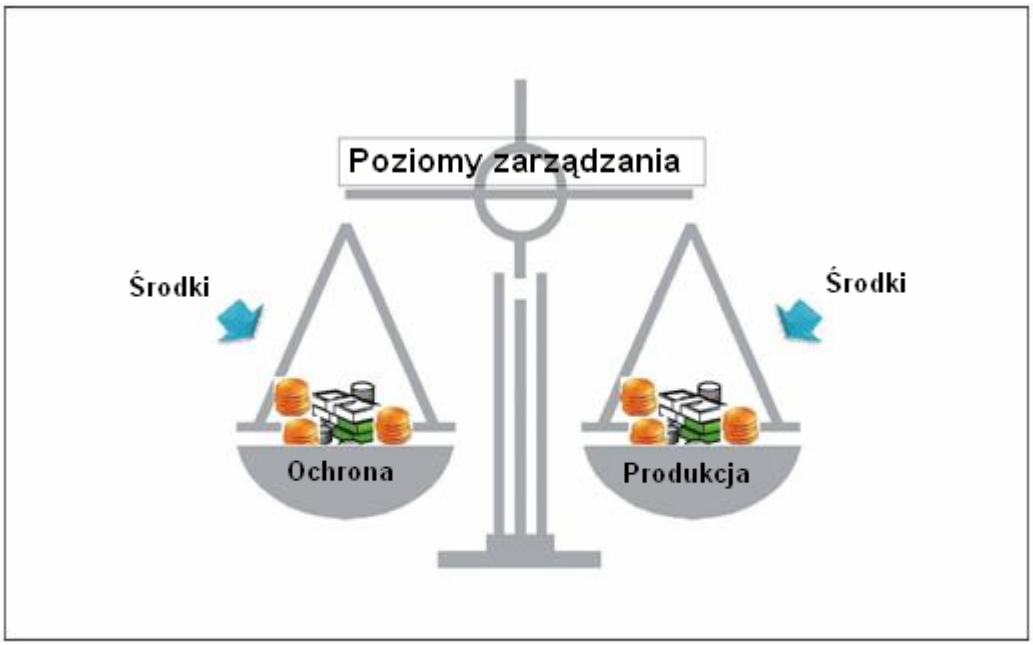
3.3.2 Środki dostępne dla organizacji lotniczych są ograniczone. Nie ma żadnej organizacji lotniczej o nieograniczonych środkach finansowych. Są one konieczne do prowadzenia podstawowych funkcji biznesowych organizacji, które bezpośrednio i pośrednio wspierają świadczenie usług. Rozmieszczanie środków staje się zatem jednym z najważniejszych, jeśli nie najważniejszym, z procesów organizacyjnych, za które jest odpowiedzialne wyższe kierownictwo.

3.3.3 O ile pogląd o zarządzaniu bezpieczeństwem jako podstawową funkcją biznesu nie jest stosowany przez organizację, istnieje możliwość szkodliwego współzawodnictwa w rozmieszczaniu środków przy spełnianiu podstawowych funkcji, które bezpośrednio lub pośrednio wspierają świadczenie usług. Takie współzawodnictwo może prowadzić do problemu związanego z zarządzaniem, który został nazwany „dylemat dwóch P” [ang. **Protection, Production**].

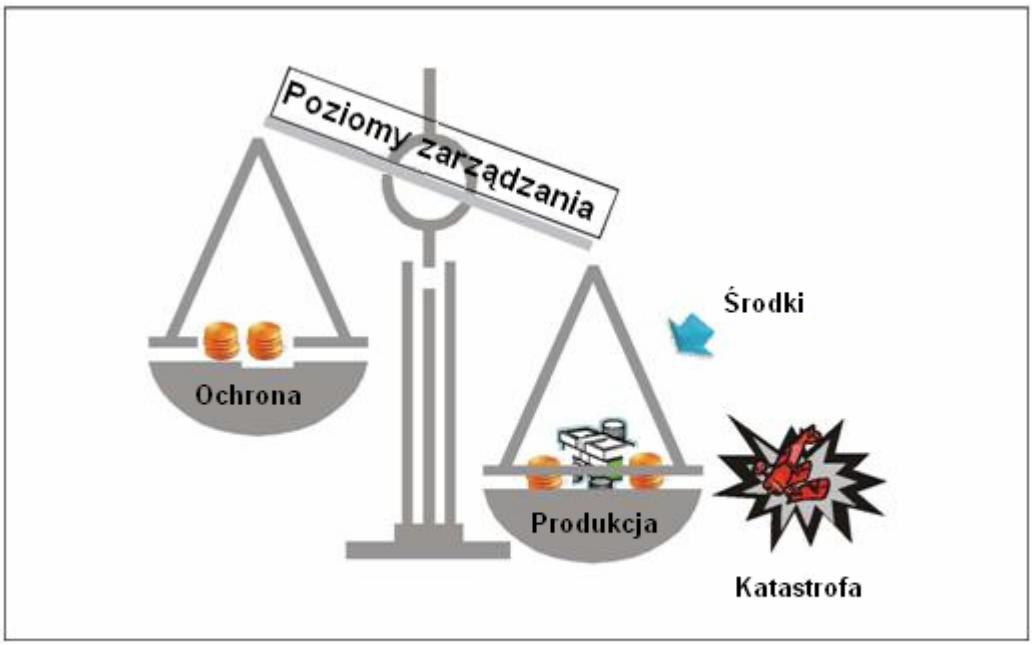
3.3.4 Najprościej mówiąc „dylemat dwóch P” może być scharakteryzowany jako konflikt, który może narodzić się na poziomie wyższego kierownictwa organizacji, ponieważ pogląd, iż środki muszą być rozmieszczane na albo/lub podstawie tego, co jest uważane za sprzeczne cele: cele produkcji (świadczenia usług) lub cele ochrony (bezpieczeństwo).

3.3.5 Ilustracja 3-1A pokazuje zrównoważone rozmieszczenie środków na cele produkcji i ochrony, które jest rezultatem organizacyjnych procesów decyzyjnych w oparciu o zarządzanie bezpieczeństwem jako podstawowej funkcji biznesu (kolejnej podstawowej funkcji). Ponieważ zarządzanie bezpieczeństwem jest uważane za kolejny proces organizacyjny oraz kolejną podstawową funkcję biznesu, bezpieczeństwo i wydajność nie stanowią konkurencji, lecz są blisko ze sobą powiązane. To skutkuje zrównoważonym rozmieszczeniem środków przez organizację w celu zapewnienia jej ochrony podczas produkcji. W tym przypadku „dylemat dwóch P” zostaje skutecznie rozwiązany. W istocie można dyskutować czy w takim razie dylemat ten w ogóle istnieje.

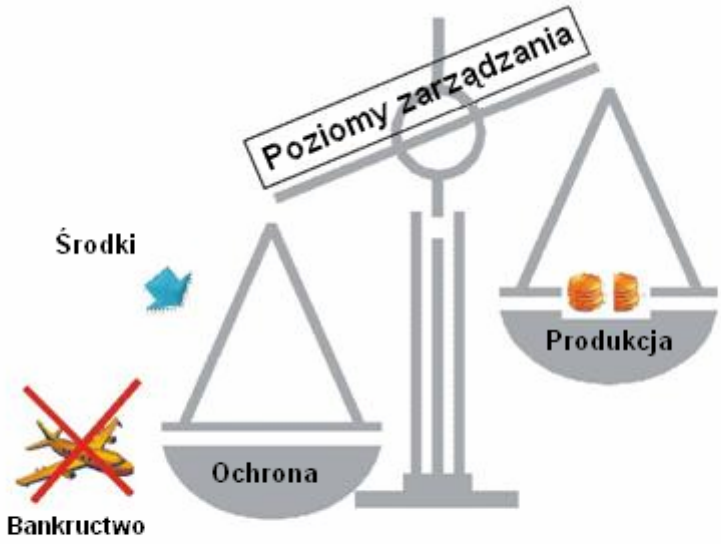
3.3.6 Niestety historia lotnictwa pokazuje, że skuteczne rozwiązanie tej kwestii nie jest powszechnym zjawiskiem. Historia pokazuje raczej tendencję organizacji w kierunku zakłócania równowagi pomiędzy rozmieszczeniem środków, ze względu na perspektywę współzawodnictwa pomiędzy produkcją a ochroną. W przypadkach, w których takie współzawodnictwo się rozwija, przegrywa zwykle ochrona, bo organizacje uprzywilejowują cele produkcyjne (jednak wprowadzając wiele sprzecznych ze sobą zastrzeżeń). Nieuchronnie, jak pokazuje ilustracja 3-1B, takie stronnicze decydowanie organizacji prowadzi do katastrofy. Pozostaje to tylko kwestią czasu.




Ilustracja 3 - 1A. Dylemat zarządzania




Ilustracja 3 - 1B. Dylemat zarządzania




**Ilustracja 3 - 1C. Dylemat zarządzania**

3.3.7 Ilustracja 3-1C ukazuje alternatywę w stosunku do stronniczego rozmieszczania środków omówionego w dwóch poprzednich paragrafach. W tym przypadku uprzywilejowanie rozmieszczenia tych środków zmierza w kierunku ochrony, co prowadzi do bankructwa. Chociaż takiego rozwiązania trudno doszukać się w kronikach lotnictwa, mimo to uzmysławia ono znaczenie rozważnego decydowania organizacji w odniesieniu do rozmieszczania środków. W końcowej analizie jest jasne, że ewolucja „dylematu dwóch P" jest zanegowana przez stanowisko koncentrujące się na zarządzaniu bezpieczeństwem jako podstawową funkcją biznesu na tym samym poziomie, przywiązując tę samą wagę co do innych podstawowych procesów w biznesie. W ten sposób zarządzanie bezpieczeństwem staje się częścią struktury organizacji zapewniając rozmieszczenie środków współmierne z sumą zasobów dostępnych organizacji.

3.3.8 Uzasadnienie zarządzania bezpieczeństwem jako podstawowej funkcji biznesu może zostać poszerzone o ostateczny argument, który ma poważne znaczenie dla procesu stanowiącego podstawę identyfikacji ryzyka oraz zarządzanie ryzykiem jako czynności operacyjnych wraz z funkcjami związanymi z zarządzaniem bezpieczeństwem (omawiane w rozdziałach 4 i 5).

3.3.9 Odkąd organizacje lotnicze za swój główny cel stawiają świadczenie usług, robienie tego efektywnie i na czas może niekiedy pozostawać w konflikcie z operacyjnymi względami bezpieczeństwa. Na przykład, ze względu na wymaganie zgodności z rozkładem lotów, przewoźnik musi lądować na konkretnym lotnisku o konkretnej godzinie, bez względu na warunki pogodowe, natężenie ruchu, ograniczenia na lotnisku i inne podobne kwestie, które są nierozerwalnie związane ze świadczeniem usług. Jeśli względy wydajności świadczenia usług (wymóg zgodności z planem lotów) zostałyby usunięte, bezpieczeństwo operacyjne (niesprzyjające warunki pogodowe, wysokie natężenie ruchu, ograniczenia na lotnisku) przestałoby mieć znaczenie. Lot byłby kontynuowany tylko wtedy, gdy zniknęłyby ograniczenia. To jednakże jest niepraktyczne, ponieważ zniszczyłoby opłacalność branży lotniczej. Operacje lotnicze muszą być zatem prowadzone pod warunkami, które dyktują nie tyle względy bezpieczeństwa operacyjnego, co raczej wymogi świadczenia usług.

3.3.10 Powiązanie jest wyraźne: zagadnienia bezpieczeństwa lotniczego nie są właściwym ani naturalnym warunkiem operacji lotniczych, lecz dodatkowymi kwestiami związanymi z zaangażowaniem się w czynności związane z produkcją i świadczeniem usług. To wzmacnia potrzebę zarządzania bezpieczeństwem jako podstawową funkcją biznesu, która zapewnia analizę zasobów organizacji i jej celów oraz pozwala na zrównoważone i realistyczne rozmieszczenie środków pomiędzy celami ochrony i produkcji, co ogólnie wspiera świadczenie usług przez organizację.

### 3.4 POTRZEBA ZARZĄDZANIA BEZPIECZEŃSTWEM

3.4.1 Tradycyjnie potrzeba zarządzania bezpieczeństwem była uzasadniana przewidywanym rozwojem branży oraz potencjalnym wzrostem liczby wypadków jako konsekwencji tego rozwoju. Podczas gdy zmniejszanie ilości wypadków zawsze pozostanie priorytetem lotnictwa, są ważniejsze czynniki, niż przewidywania statystyczne leżące u podstaw przejścia do stworzenia obszaru zarządzania bezpieczeństwem w międzynarodowym lotnictwie cywilnym na całym świecie.

3.4.2 Lotnictwo jest prawdopodobnie najbezpieczniejszym środkiem masowego transportu i jednym z najbezpieczniejszych socjotechnicznych wynalazków w historii ludzkości. To osiągnięcie ma szczególną wartość, biorąc pod uwagę jak młoda jest branża lotnicza, mierzona w dekadach w porównaniu do innych branż, których historie rozciągają się na stulecia. To hołd dla społeczności zarządzającej bezpieczeństwem lotnictwa i jej nieustannych wysiłków, by w ciągu zaledwie stulecia w historii transportu lotnictwo rozwinęło się z niezadowalającego systemu do systemu ultra bezpiecznego. Z perspektywy czasu historia rozwoju niezawodności bezpieczeństwa lotniczego może być podzielona (tak jak ewolucja myślenia o bezpieczeństwie omawiana w rozdziale 2) na trzy różne okresy, każdy o zupełnie różnych cechach.

3.4.3 W pierwszym okresie, który rozciąga się od pionierskich lat u progu XX wieku do późnych lat 60-tych (epoka techniczna omawiana w rozdziale 2), lotnictwo może być scharakteryzowane jako kruchy system z punktu widzenia niezawodności bezpieczeństwa. Zagrożenia bezpieczeństwa, choć z pewnością niecodzienne, nie należały do rzadkości. Było więc logiczne, że rozumienie bezpieczeństwa oraz strategie zapobiegania wypadkom opracowywano głównie na podstawie badań nad wypadkami. Nie istniał właściwie żaden system bezpieczeństwa, to raczej branża funkcjonowała dzięki jednostkom, które zapewniały jej postęp. Skoncentrowanie na bezpieczeństwie leżało w gestii pojedynczych osób i indywidualnego zarządzania ryzkiem w systemie bezpieczeństwa, które z kolei zostało zbudowane dzięki intensywnym programom szkoleniowym.

3.4.4 W drugim okresie, od wczesnych lat 70-tych do połowy lat 90-tych lotnictwo stało się nie tylko po prostu systemem, lecz systemem bezpiecznym. Częstotliwość załamania się systemu bezpieczeństwa radykalnie zmalała i stopniowo rozwinęło się bardziej całościowe rozumienie bezpieczeństwa, które wyszło poza rozpatrywanie szerszego systemu przez pojedyncze jednostki. To spowodowało w sposób naturalny poszukiwania wiedzy na temat bezpieczeństwa opartego nie tylko na badaniach nad wypadkami, ale także spowodowało przesunięcie w kierunku badań nad incydentami. Wspomnianemu przesunięciu w stronę szerszej perspektywy dotyczącej spraw bezpieczeństwa i badań nad incydentami towarzyszyło intensywne wprowadzanie technologii (jako jedynej drogi do osiągnięcia wzrostu wymaganego w systemie produkcji) oraz następująca po nim wielokrotna aktualizacja dodatkowych regulacji dotyczących bezpieczeństwa.

3.4.5 Od połowy lat 90-tych do dziś, lotnictwo weszło w trzeci okres niezawodności bezpieczeństwa, stając się ultra bezpiecznym systemem (to jest systemem, w którym zdarza się mniej niż jedno załamanie bezpieczeństwa [katastrofa] na każdy milion cykli produkcyjnych [lotów]). Z globalnego punktu widzenia, pomimo lokalnych zakłóceń, wypadki stały się na tyle rzadkie, że można je uznać za anomalie w systemie. Poważnych incydentów również jest mniej i występują coraz rzadziej. Wraz ze zmniejszaniem się liczby wypadków i incydentów nastąpiło przesunięcie w kierunku szerszej perspektywy bezpieczeństwa systemowego, które to przesunięcie rozpoczęte w poprzednim okresie urzeczywistniło się obecnie. Podstawowym czynnikiem tej zmiany było zaadaptowanie postawy biznesowej w zarządzaniu bezpieczeństwem, opartej na rutynowym zbieraniu i analizie codziennych danych operacyjnych. To biznesowe podejście do bezpieczeństwa leży u podstaw uzasadnienia dla systemu zarządzania bezpieczeństwem (SMS) omawianego w rozdziale 7. Najprościej rzecz ujmując, SMS jest zastosowaniem praktyk związanych z zarządzaniem biznesem w zarządzaniu bezpieczeństwem. Ilustracja 3-2 pokazuje omówioną powyżej ewolucję bezpieczeństwa.

3.4.6 Zastosowanie praktyk zarządzania biznesem w bezpieczeństwie lotniczym, z leżącym u jego podstaw rutynowym zbieraniem i analizą danych operacyjnych, ma na celu rozszerzenie obszaru bezpieczeństwa omówionego w rozdziale 2. W ramach tego obszaru organizacja może swobodnie poruszać się świadcząc swoje usługi, z zapewnieniem, że jest to przestrzeń maksymalnej odporności na ryzyko jako konsekwencji zagrożeń, które istnieją w środowisku, w jakim te organizacje muszą funkcjonować by świadczyć swe usługi.

3.4.7 Omówiono już znaczenie zrównoważonego podziału środków w dążeniu do osiągania celów ochrony i produkcji, dla rozwiązania „dylematu dwóch P". Jako rozwinięcie tej kwestii istotne są również pojęcia produkcji i ochrony do zdefiniowania granic przestrzeni bezpieczeństwa organizacji, jak pokazano na ilustracji 3-3.

3.4.8 W rozdziale będzie jeszcze mowa o tym, że podjęcie decyzji o nadmiernym alokowaniu zasobów na kwestie bezpieczeństwa może, teoretycznie, doprowadzić organizację do bankructwa. Dlatego tak istotnym jest określenie granic, które staną się systemem wczesnego ostrzegania jeżeli organizacja zbliży się do nich w wyniku niezrównoważonego przydzielania zasobów. Powstaną niejako dwie strony graniczne: granica finansowa i granica utraty bezpieczeństwa.

3.4.9 Zarząd określa granice finansowe organizacji. Pracując nad systemem wczesnego ostrzegania przed zbliżającą się granicą wypłacalności, zarząd nie bierze pod uwagę najgorszego możliwego rozstrzygnięcia (bankructwa). Praktyki zarządu są oparte na codziennym zbieraniu i analizie określonych wskaźników finansowych: trendów rynkowych, zmian cen towarów oraz zewnętrznych zasobów potrzebnych organizacji do świadczenia usług. Czyniąc to zarząd finansowy nie tylko definiuje granicę finansową obszaru bezpieczeństwa, lecz także wciąż na nowo ustala jej pozycję.

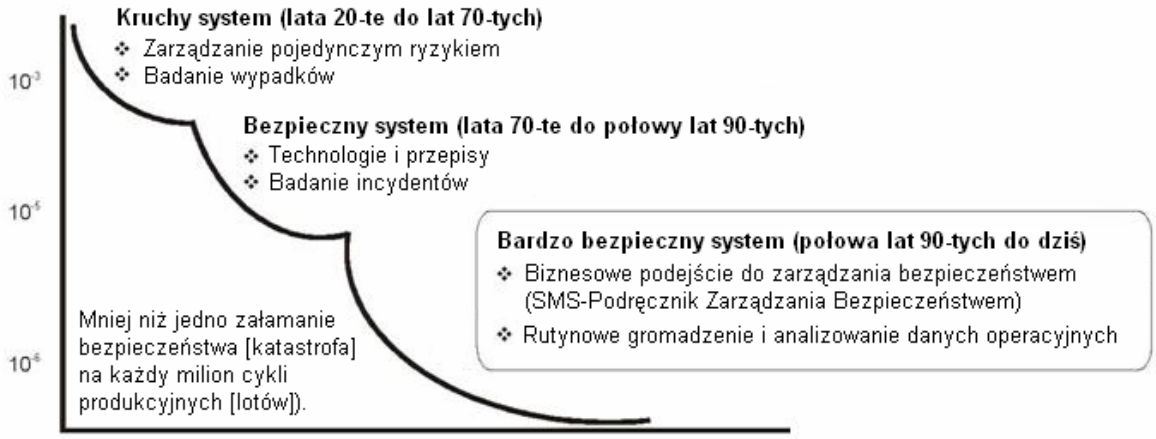
3.4.10 Należy tu również przypomnieć, że decyzje organizacji prowadzące do przydzielania zbyt dużych środków na cele produkcji mogą mieć wpływ na wyniki w zakresie bezpieczeństwa, co może w końcu prowadzić do katastrofy. Dlatego niezbędne jest określenie granicy bezpieczeństwa, która ostrzegałaby odpowiednio wcześnie, że rozwija się lub ma miejsce sytuacja niezrównoważonego przydzielenia środków, w tym przypadku na rzecz ochrony. Granica w obszarze bezpieczeństwa powinna być określona przez zarząd organizacji.

3.4.11 Granica ta jest niezbędna by ostrzegać organizację o tym, że niezrównoważone rozmieszczenie środków, które uprzywilejowuje cele produkcyjne, może prowadzić do katastrofy. Niestety nie ma analogii pomiędzy praktykami, które wdrażane są w ramach zarządzania finansami i zarządzania bezpieczeństwem. Ze względu na głęboko zakorzeniony pogląd o bezpieczeństwie jako o braku wypadków lub poważnych incydentów, granica w obszarze bezpieczeństwa występuje w organizacjach lotniczych rzadko. W istocie, można się spierać czy chociaż nieliczne organizacje lotnicze, jeśli w ogóle jakiekolwiek, rzeczywiście zbudowały obszar bezpieczeństwa.

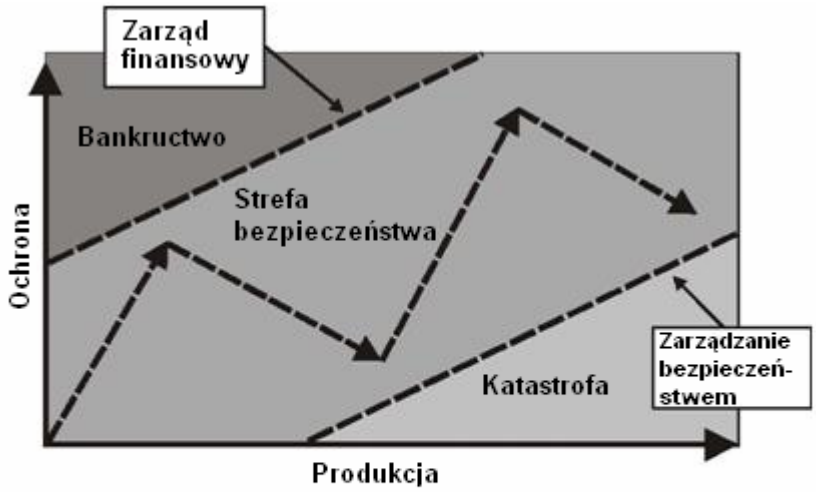
3.4.12 Chociaż istnieje system wczesnego ostrzegania w zakresie bezpieczeństwa, jest on zazwyczaj ignorowany i nie uznawany, a organizacje dowiadują się, że mają nierównomiernie rozmieszczone środki dopiero wówczas, gdy ma miejsce wypadek lub poważny incydent. W ten sposób, w odróżnieniu od zarządzania finansami, w perspektywie bezpieczeństwa jako braku wypadków lub poważnych incydentów, organizacja wyszukuje najgorszy przypadek (lub jego brak) jako wskaźnik jej pomyślnego zarządzania bezpieczeństwem.

3.4.13 Ewolucja niezawodności w zakresie bezpieczeństwa omówiona w podrozdziałach od 3.4.3 do 3.4.5 dowodzi potrzeby rozwijania dodatkowych, alternatywnych środków zbierania danych dotyczących bezpieczeństwa, poza raportami o wypadkach i incydentach. Do lat 70-tych zbieranie danych dotyczących bezpieczeństwa odbywało się głównie poprzez badania nad wypadkami i incydentami i stało się stopniowo niedostateczne, gdy ulepszenia w zakresie bezpieczeństwa doprowadziły do redukcji liczby wypadków. Ponadto, jeśli chodzi o pozyskiwanie danych dotyczących bezpieczeństwa, proces badania wypadków i poważnych incydentów jest reaktywny: potrzebuje bodźca (załamania się bezpieczeństwa), żeby uruchomić proces zbierania danych dotyczących bezpieczeństwa.

3.4.14 Jako konsekwencję potrzeby utrzymania stałego zasobu danych o bezpieczeństwie, dane z wypadków i poważnych incydentów zostały uzupełnione o dane z rozbudowanych systemów zbierania danych. W rozbudowanych systemach, dane o bezpieczeństwie z mniej poważnych incydentów stały się dostępne poprzez obligatoryjne i dobrowolne programy raportowania. W kwestii pozyskiwania danych o bezpieczeństwie, te nowsze systemy są prewencyjne - odkąd incydenty uruchamiające proces zbierania danych o bezpieczeństwie mają znacząco mniejsze konsekwencje niż te, które uruchamiają proces zdobywania danych o bezpieczeństwie z wypadków i poważnych incydentów. Mimo to pozostaje faktem, że dane o bezpieczeństwie z programów informowania stają się dostępne tylko wówczas, kiedy niedociągnięcia powodują jakiś incydent.




**Ilustracja 3 - 2. Pierwszy bardzo bezpieczny sytem**




Źródło: James Reason

**Ilustracja 3 - 3. Strefa bezpieczeństwa**

3.4.15 Do początku lat 90-tych stało się oczywiste, iż aby utrzymać bezpieczeństwo w ultra bezpiecznym systemie i wspierać biznesowe podejście do bezpieczeństwa leżące u podstaw SMS, potrzebne są większe ilości danych, zdobywanych bez potrzeby dodatkowych bodźców. To doprowadziło do rozwoju systemów zbierania danych o bezpieczeństwie o charakterze prognozującym, jako uzupełnienie systemów zbierania danych o bezpieczeństwie o charakterze prewencyjnym i reaktywnym. Do tego celu zostały wprowadzone systemy elektronicznego pozyskiwania danych oraz samoraportujące programy o operacjach bez ryzyka, w celu gromadzenia danych dotyczących bezpieczeństwa z normalnych operacji, bez zdarzeń inicjujących proces zbierania danych o bezpieczeństwie. Najnowszym dodatkiem do systemów zbierania danych o bezpieczeństwie o charakterze prognozującym są systemy oparte na bezpośredniej obserwacji personelu podczas zwykłych operacji.

3.4.16 Zbieranie danych dotyczących bezpieczeństwa ze zwykłych operacji lotniczych jest mocno uzasadnione. System lotniczy, tak jak każdy system wynaleziony przez człowieka, mimo swojej doskonałości w zakresie bezpieczeństwa, jest daleki od perfekcji. Lotnictwo to system otwarty; działa w niekontrolowanym, naturalnym środowisku i stanowi podmiot zakłóceń, które występują w środowisku. Niemożliwe jest stworzenie od podstaw otwartego systemu, który byłby doskonały tylko z tego względu, że nie sposób przewidzieć wszystkich możliwych interakcji pomiędzy ludźmi, technologią, a także kontekstem, w którym operacje lotnicze mają miejsce. Monitorowanie operacji w czasie rzeczywistym pozwala na identyfikację i poprawę wad i usterek, które nie zostały przewidziane podczas projektowania systemu. Ten argument zostanie szerzej rozwinięty w podrozdziałach od 3.4.17 do 3.4.19.

**„Odchylenie praktyczne”**

3.4.17 Podczas wczesnych stadiów projektowania systemu, projektanci systemu mają na uwadze dwa najważniejsze pytania, biorąc pod uwagę deklarowane cele produkcyjne systemu:

a) jakie środki są niezbędne, by osiągnąć takie cele produkcyjne? oraz

b) jak system może być chroniony przed ryzykiem podczas operacji koniecznych do osiągnięcia założonych celów produkcyjnych?

Projektanci systemu stosują różne metody, by odpowiedzieć na te pytania. Jedną z takich metod jest określenie prawdopodobnych scenariuszy (tak wielu jak to tylko możliwe) interakcji operacyjnych pomiędzy ludźmi, technologią i kontekstem operacyjnym, żeby zidentyfikować potencjalne ryzyko podczas operacyjnych interakcji.

3.4.18 Rezultatem tego procesu jest wstępny projekt systemu oparty na trzech podstawowych założeniach: technologia potrzebna do osiągnięcia celów produkcyjnych systemu, szkolenie niezbędne do właściwego posługiwania się technologią oraz przepisy i procedury, które regulują działanie systemu i ludzkich zachowań. Te założenia składają się na podstawowe (lub idealne) działanie systemu. Na potrzeby wyjaśnienia idealnego lub podstawowego działania systemu (czyli jak system powinien działać) może on być przedstawiany graficznie jako linia prosta (ilustracja 3-4).

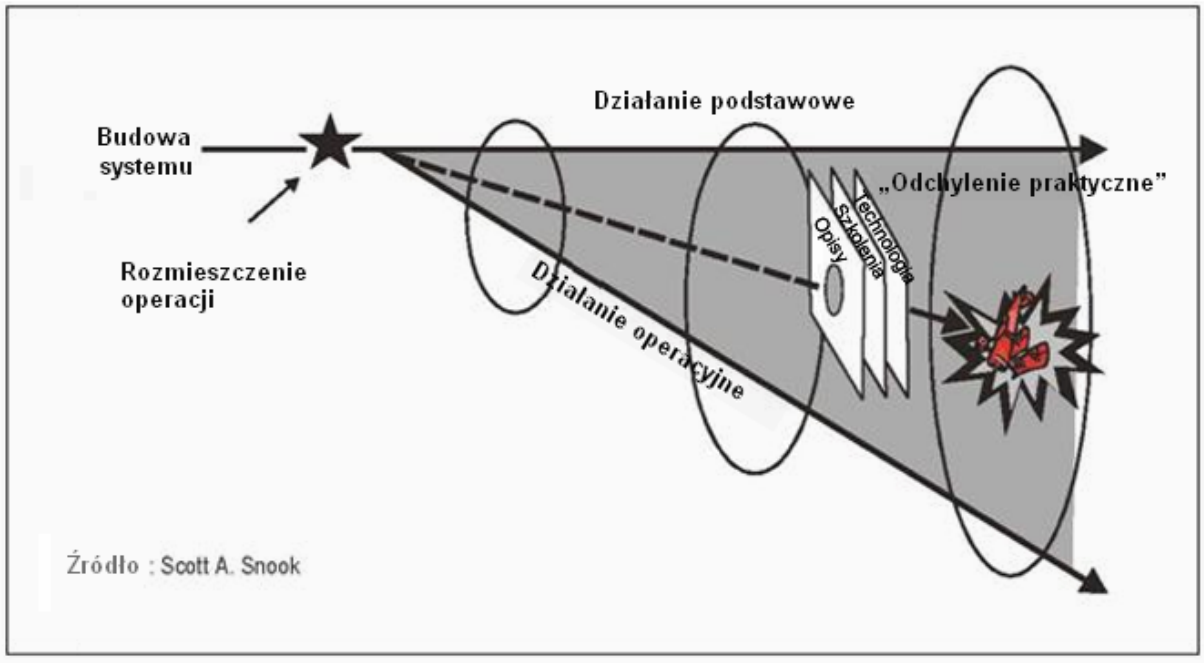
3.4.19 Założenia są testowane, podstawowe działanie uprawomocnione, w końcu system staje się operacyjnym. Gdy już zostanie wdrożony, system działa tak jak został zaprojektowany, czyli według podstawowych założeń. Zwykle jednak działanie operacyjne jest różne od działania podstawowego. Innymi słowy, gdy systemy stają się operacyjne, pojawia się stopniowo tendencja do odchodzenia od działania podstawowego, założonego pierwotne, w kierunku stopniowego lecz konsekwentnego rozwijania systemu operacyjnego jako konsekwencji operacji w rzeczywistości. Z chwilą gdy ta tendencja jest konsekwencją praktyki dnia codziennego jest ona nazywana „odchyleniem praktycznym”.

3.4.20 Praktyczne odchylenie od działania podstawowego w stronę działania operacyjnego jest nieuniknione w każdym systemie, bez względu na to jak uważne i dobrze przemyślane było planowanie projektu. Przyczyny odchylenia praktycznego są złożone: technologia nie zawsze działa zgodnie z prognozami, procedury nie mogą być przeprowadzone tak, jak zaplanowano w dynamicznych warunkach operacyjnych; przepisy nie uwzględniają ograniczeń wynikających z kontekstu; wprowadzanie drobnych zmian do systemu po jego zaprojektowaniu bez równoczesnej ponownej oceny ich wpływu na podstawowe założenia projektu; uzupełnienie o nowe składniki systemu bez właściwej oceny z punktu widzenia zagrożeń, które te składniki mogą wprowadzać; interakcja z innymi systemami i tak dalej. Tak więc właściwym jest stwierdzenie, że w każdym systemie działalność człowieka jest skierowana na świadczenie usług w obrębie tego odchylenia.

3.4.21 Ujęcie tego, co dzieje się w ramach odchylenia praktycznego poprzez środki formalne (na przykład formalne uchwycenie w ramy ekspertyzy) niesie ze sobą poważny potencjał wiedzy o pomyślnym dostosowaniu do wymogów bezpieczeństwa i także kontroli nad ryzkiem. Formalne uchwycenie w ramy ekspertyzy może być zamienione w formalne interwencje w celu przeprojektowania lub wprowadzenia ulepszeń, jeśli potencjał wiedzy zostaje wprowadzony w sposób odgórny. Minus stanowi fakt, że niesprawdzone namnożenie się lokalnych dostosowań i personalnych strategii może spowodować, że odchylenie praktyczne odbiegnie za bardzo w stosunku od założonego działania podstawowego, do tego stopnia, że może dojść do incydentu lub wypadku. Ilustracja 3-4 pokazuje pojęcie odchylenia praktycznego omówionego w tym paragrafie.

## 3.5 STRATEGIE ZARZĄDZANIA BEZPIECZEŃSTWEM

3.5.1 Wystąpienie „odchylenia praktycznego" jest nieuniknione. Wszystkie organizacje lotnicze, nawet te najpewniejsze finansowo, najbardziej prężne przeprowadzają swoje operacje w obrębie „odchylenia praktycznego". „Odchylenie praktyczne" leży w samej naturze dynamicznych i otwartych socjotechnicznych systemów produkcji, wśród których lotnictwo jest najważniejszym przykładem. Na co dzień podczas świadczenia usług, organizacje sterują „odchyleniem praktycznym", starając się usytuować jak najdalej od punktu, w którym to odchylenie jest największe i możliwie jak najbliżej punktu, w którym to odchylenie się pojawia. Podczas tych codziennych działań organizacje muszą powstrzymać potencjalne przeciwne „prądy" i przeszkody: są to zagrożenia, które powstają jako konsekwencja niezrównoważonego rozmieszczenia środków w celu wspierania potrzeb organizacji oraz nierozwiązanie „dylematu dwóch P".



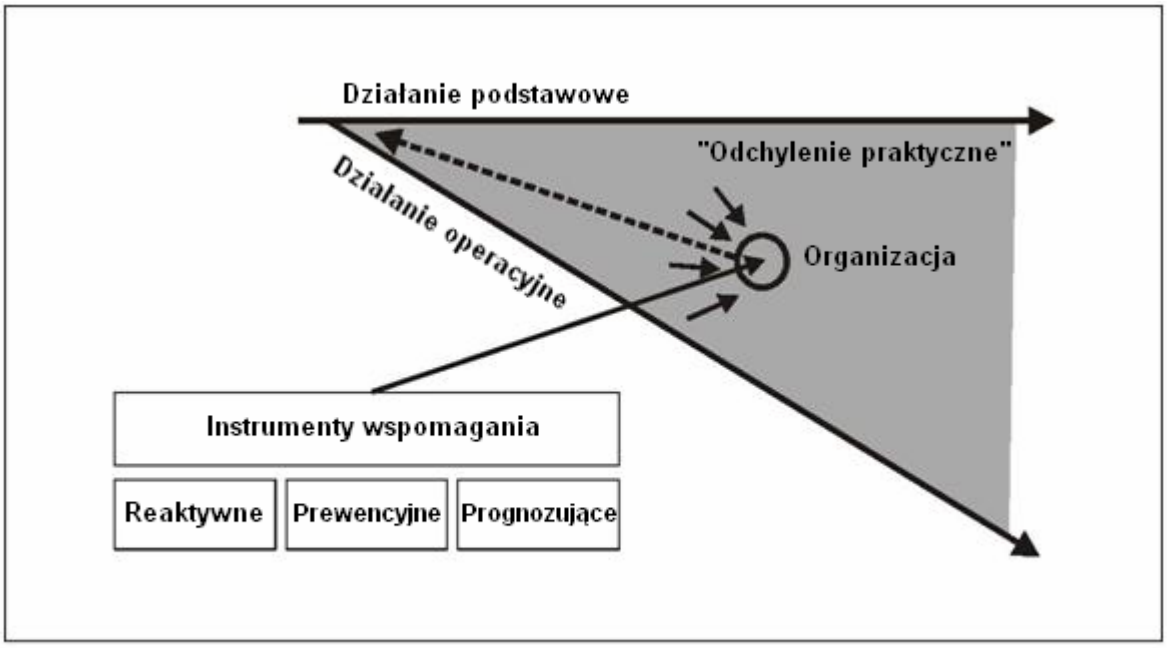

Ilustracja 3 - 4. "Odchylenie praktyczne"

3.5.2 W celu pomyślnego kierowania „odchyleniem praktycznym" organizacje potrzebują instrumentów wspomagania, które wygenerują potrzebne informacje, aby omijać trudności i przeszkody (patrz ilustracja 3-5). Owe instrumenty wspomagania zbierają dane operacyjne tak, że kiedy zostaną one przeanalizowane, będą informowały organizacje o najlepszych sposobach omijania trudności i przeszkód. Jest wiele instrumentów wspomagania dostępnych dla organizacji lotniczych. Mogą one zostać podzielone na trzy typy: reaktywne, prewencyjne i prognozujące, w zależności od wagi zdarzenia, które spowodowało proces zbierania danych o bezpieczeństwie.

3.5.3 Reaktywne instrumenty wspomagania wymagają bardzo poważnego wydarzenia inicjującego proces zbierania danych o bezpieczeństwie. Reaktywne instrumenty wspomagania opierają się na oczekiwaniu aż „coś się zepsuje, by móc to naprawić". Są one najodpowiedniejsze w sytuacjach błędów technologii i/lub niezwykłych zdarzeń. Reaktywne instrumenty wspomagania są integralną częścią rozwiniętego zarządzania bezpieczeństwem. Mimo to wkład, jaki reaktywne instrumenty wspomagania mają w zarządzanie bezpieczeństwem zależy od zakresu, w jakim informacje, które te instrumenty wytwarzają, wychodzą poza wywołującą przyczynę (przyczyny) zdarzenia, a także od ustalenia winy oraz zawierają przyczyny i ustalenia dotyczące ryzyka. Badanie wypadków oraz poważnych incydentów to przykłady reaktywnych instrumentów wspomagania.

3.5.4 Prewencyjne instrumenty wspomagania wymagają znacznie mniej poważnego i o mniejszych konsekwencjach zdarzenia inicjującego proces zbierania danych o bezpieczeństwie. Prewencyjne instrumenty wspomagania są oparte na założeniu, że błędy systemu mogą być zminimalizowane poprzez identyfikowanie ryzyka w ramach systemu zanim on zawiedzie oraz podejmowanie czynności potrzebnych do łagodzenia takiego ryzyka. Przykładami prewencyjnych instrumentów wspomagania są obowiązkowe i dobrowolne systemy raportowania, audyty bezpieczeństwa oraz przeglądy stanu bezpieczeństwa.

3.5.5 Prognozujące instrumenty wspomagania nie wymagają wydarzenia inicjującego proces zbierania danych o bezpieczeństwie. Rutynowe dane operacyjne są gromadzone w sposób ciągły, w czasie rzeczywistym. Prognozujące instrumenty wspomagania nawigacji są oparte na pojęciu mówiącym, że zarządzanie bezpieczeństwem jest najlepsze wtedy, gdy szuka się problemu, a nie czeka aż on pojawi się sam. Dlatego prognozujące systemy zbierania danych o bezpieczeństwie usilnie poszukują informacji, które mogą wskazywać zbliżające się z różnych stron ryzyko.




Ilustracja 3 - 5. Sterowanie "Odchyleniem praktycznym"

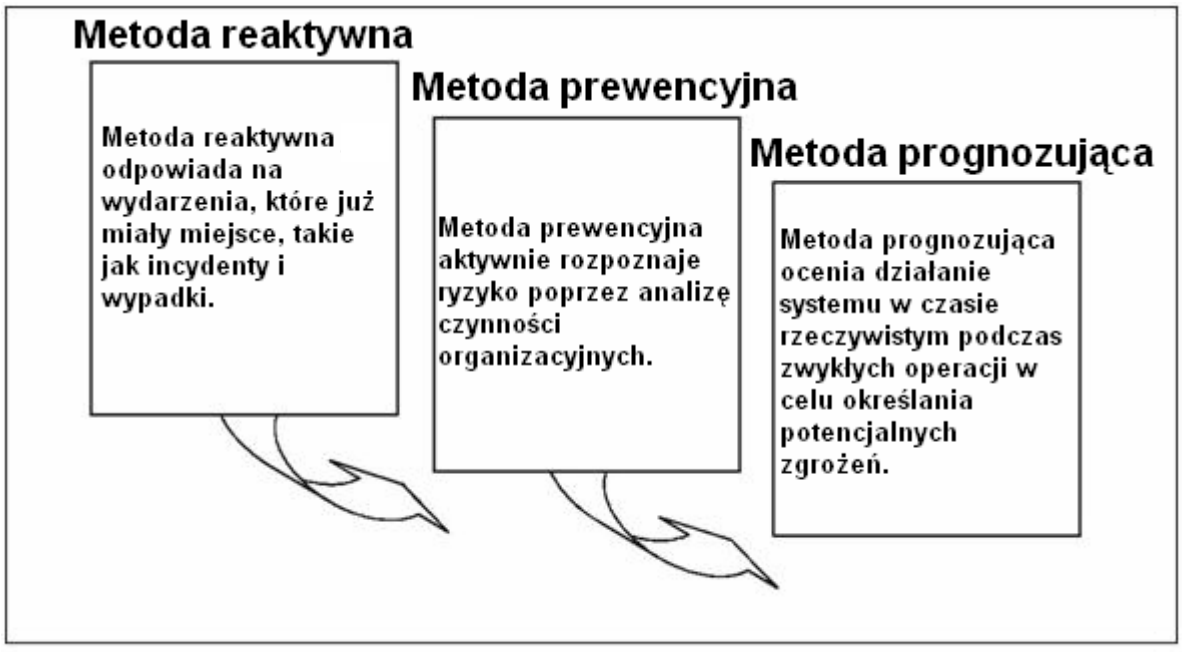
3.5.6 Prognozujące systemy zbierania danych są w istocie systemami statystycznymi, dzięki czemu znaczna ilość danych operacyjnych, które same w sobie są bez znaczenia, zostaje zebrana i przeanalizowana, a następnie połączona z reaktywnymi i prewencyjnymi systemami zbierania danych. Nagromadzenie danych prowadzi zatem do stworzenia kompletnego zasobu wiedzy, która pozwala organizacjom poruszać się wśród przeszkód i trudności oraz przyjąć optymalną postawę wobec „odchylenia". Przykładami prognozujących instrumentów wspomagania są systemy informowania o ryzyku, analiza danych lotu oraz zwykłe monitorowanie operacji.

3.5.7 Reaktywne, prewencyjne oraz prognozujące systemy zbierania danych o bezpieczeństwie dostarczają danych o bezpieczeństwie dla odpowiadających im reaktywnych, prewencyjnych i prognozujących strategii zarządzania bezpieczeństwem, które z kolei służą reaktywnym, prewencyjnym oraz prognozującym

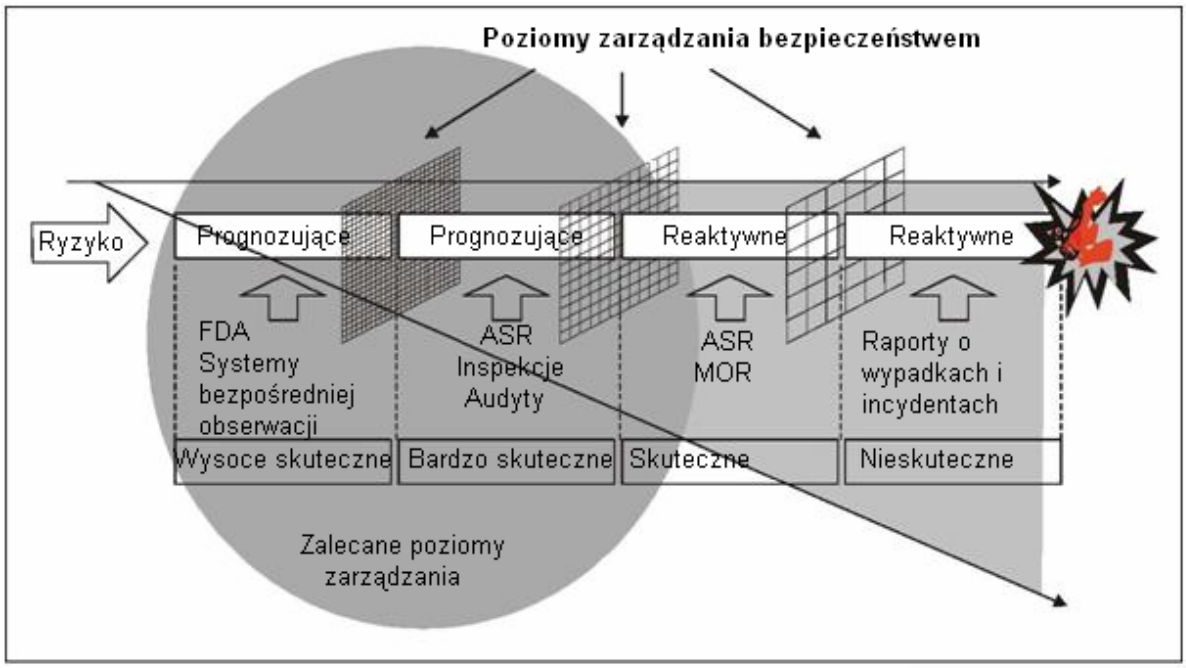
metodom łagodzenia ryzyka. Podsumowanie strategii zarządzania bezpieczeństwem, tak jak je omówiono w poprzednim paragrafie, pokazuje ilustracja 3-6.

3.5.8 Dojrzałe zarządzanie bezpieczeństwem wymaga integracji reaktywnych, prewencyjnych oraz prognozujących systemów gromadzenia danych o bezpieczeństwie, rozsądnego połączenia reaktywnych, prewencyjnych oraz prognozujących strategii łagodzenia ryzyka, a także rozwoju reaktywnych, prewencyjnych i przewidujących metod łagodzenia ryzyka. Oprócz tego należy mieć na uwadze podczas budowania strategii łagodzenia, że każdy z trzech dotychczas omówionych systemów pozyskiwania danych o bezpieczeństwie gromadzi dane na różnych poziomach trendów operacyjnych. Tak samo ważne jest, aby każda z trzech strategii i metod łagodzenia była wdrażana na różnych poziomach „odchylenia praktycznego".

3.5.9 W celu zilustrowania wspomnianych kwestii należy powrócić do „odchylenia praktycznego", jak pokazano na ilustracji 3-7. Ryzyko stanowi kontinuum wzdłuż całej linii „odchylenia praktycznego". Jeśli ryzyko nie zostanie powstrzymane, to narasta wraz z „odchyleniem praktycznym" i niesie w sobie wzrastający potencjał zniszczeń. Blisko punktu, w którym pojawia się „odchylenie praktyczne" ryzyko jest relatywnie małe, ponieważ nie ma możliwości rozwinięcia swojego niszczącego potencjału. Im bardziej niepowstrzymany wzrost ryzyka wzdłuż „odchylenia praktycznego", tym większego nabiera rozpędu i wzrasta jego niszczący potencjał. Wtedy, gdy ryzyko dochodzi do punktu, w którym „odchylenie praktyczne" jest najszersze, osiąga ono maksymalny potencjał zniszczeń, włączając w to możliwe poważne uszkodzenia. Dlatego tak istotne dla zarządzania bezpieczeństwem jest zlokalizowanie ryzyka możliwie blisko punktu początkowego „odchylenia praktycznego".




Ilustracja 3 - 6. Strategie zarządzania bezpieczeństwem




**Ilustracja 3 - 7. Strategie - Poziomy i narzędzia interwencji**

3.5.10 Prognozujące systemy gromadzenia danych, strategie i metody są efektywne blisko punktu powstania i początkowego narastania „odchylenia praktycznego". To daje możliwość skutecznej interwencji i wysoką wydajność. Powód, dla którego prognozujące systemy gromadzenia danych o bezpieczeństwie, strategie i metody są tak wydajne jest dwojaki: z jednej strony mają do czynienia z ryzykiem w momencie jego narodzin, uniemożliwiając rozwinięcie się jego potencjalnej szkodliwości, przez co staje się ono łatwiejsze do zlokalizowania. Dzięki temu, zmniejszenie ryzyka uzyskane na podstawie prognozujących danych o bezpieczeństwie tworzy siatkę hamującą lub filtr tak ciasny, że prawie całkowicie blokuje przeniesienie ryzyka dalej w głąb „odchylenia praktycznego".

3.5.11 Prewencyjne systemy gromadzenia danych o bezpieczeństwie, strategie i metody działają także wzdłuż „odchylenia praktycznego" i linii ryzyka, lecz nie tak blisko początku i punktu narodzin „odchylenia praktycznego" jak prognozujące systemy, strategie i metody gromadzenia danych o bezpieczeństwie. Istnieje tu również wysoki poziom bardzo wydajnej interwencji. Mimo to ryzyko może rozwinąć swój niszczący potencjał. Przez to łagodzenie ryzyka uzyskane z danych prewencyjnych stanowi siatkę hamującą i filtr, który, chociaż ciasny, pozwala na przeniknięcie rozwijającego się ryzyka w głąb „odchylenia praktycznego".

3.5.12 Reaktywne systemy, strategie i metody gromadzenia danych o bezpieczeństwie, działają na dwóch poziomach „odchylenia praktycznego". Niektóre, takie jak przymusowe systemy raportowania o zdarzeniach działają na średnim poziomie interwencji. To poziom wystarczający, ale ryzyko wciąż rozwija swój niszczący potencjał. Złagodzenia uzyskane na pierwszym poziomie reaktywnych danych o bezpieczeństwie stają się siatką i filtrem o luźnej strukturze, przez którą często może przedostać się ryzyko. Na najniższym poziomie reaktywnych systemów, strategii i metod gromadzenia danych o bezpieczeństwie, badanie wypadków i poważnych incydentów działa w trybie naprawiania szkód. Informacje wywiedzione tylko z reaktywnych danych o bezpieczeństwie są niewystarczające dla zarządzania bezpieczeństwem.

### 3.6 KONIECZNOŚĆ ZMIANY

3.6.1 Wraz z globalizacją działalności lotniczej i jej skomplikowaniem, głęboko zmienione warunki operacyjne i związane z tym nowe wyzwania powodują, że tradycyjne metody zarządzania bezpieczeństwem do pewnego akceptowalnego poziomu są mniej efektywne i wydajne. Inaczej mówiąc, potrzebny jest stały rozwój metod rozumienia i zarządzania bezpieczeństwem. Obecnie ma miejsce przemiana w międzynarodowym lotnictwie cywilnym, która odzwierciedla istotne przesunięcie od paradygmatu wypracowanego przez wysiłki z przeszłości.

3.6.2 Jak wspomniano tradycyjny paradygmat bezpieczeństwa polegał na procesie badania wypadków i poważnych incydentów jako głównych metodach i zabiegach dotyczących bezpieczeństwa i został on zbudowany na trzech założeniach:

a) System lotniczy działa przez większość czasu zgodnie z warunkami, według których został zaprojektowany (działanie podstawowe);

b) Zgodność z przepisami gwarantuje działanie podstawowe systemu i dlatego zapewnia bezpieczeństwo (oparte na zgodności);

c) Z uwagi na to, że zgodność z przepisami gwarantuje podstawowe działanie systemu, niewielkie, głównie pozbawione konsekwencji odchylenia podczas rutynowych operacji (procesy) nie mają znaczenia, tylko poważne odchylenia prowadzące do negatywnych konsekwencji (to jest rezultatów) mają znaczenie (nakierowane na wyniki).

3.6.3 Niniejszy podręcznik uprzywilejowuje powstający współcześnie, kontrastujący paradygmat bezpieczeństwa. Jest on oparty na pojęciu zarządzania bezpieczeństwem poprzez kontrolę procesu poza badaniem wypadków i również jest zbudowany na trzech podstawowych założeniach:

a) System lotnictwa nie działa przez większość czasu zgodnie z warunkami jego budowy (działanie operacyjne prowadzi do „odchylenia praktycznego”);

b) Zamiast polegać tylko na zgodności z przepisami monitoruje się działanie systemu w czasie rzeczywistym (oparcie na działaniu);

c) Odchylenia mniejsze, bez konsekwencji podczas rutynowych operacji są ciągle śledzone i analizowane (nakierowanie na proces).

### 3.7 ZARZĄDZANIE BEZPIECZEŃSTWEM – OSIEM CZĘŚCI SKŁADOWYCH

3.7.1 Proces zarządzania bezpieczeństwem opiera się na ośmiu podstawowych elementach, którymi są:

a) **Zaangażowanie się w problemy bezpieczeństwa przez wyższy zarząd organizacji**. Zarządzanie bezpieczeństwem, jak każde inne zarządzanie, wymaga przydzielania środków. Przydzielanie środków jest, jak we wszystkich organizacjach, funkcją wyższego zarządu, stąd potrzebne jest jego zaangażowanie w sprawy bezpieczeństwa. Prostymi słowy: bez pieniędzy nie ma bezpieczeństwa.

b) **Skuteczne raportowanie o bezpieczeństwie.** Znany jest aforyzm, że „nie można zarządzać tym, czego się nie zmierzy”. W celu zarządzania bezpieczeństwem organizacje muszą pozyskać dane o ryzyku, które pozwolą je zmierzyć. Większość takich danych będzie zdobywana poprzez dobrowolne osobiste raportowanie personelu operacyjnego. Dlatego istotne jest by organizacje rozwijały warunki pracy, tak, by miało miejsce skuteczne raportowanie o bezpieczeństwie personelu operacyjnego .

c) **Ciągły monitoring** poprzez systemy, które zbierają dane o ryzyku podczas zwykłych operacji. Zbieranie danych jest zaledwie pierwszym krokiem. Poza zbieraniem danych, organizacje muszą analizować i wydobywać z danych informacje o bezpieczeństwie i wiedzę na temat bezpieczeństwa, ponieważ dane zebrane i nie wykorzystywane są nieprzydatne. Dodatkowo ważne jest, by dzielić się zebranymi informacjami o bezpieczeństwie z tymi, którzy obsługują system na co dzień, bowiem te osoby, wciąż stykają się z ryzykiem, którego konsekwencje mogą zostać złagodzone dzięki skutecznemu raportowaniu o bezpieczeństwie.

d) **Badanie wypadków** mające na celu raczej identyfikację braków w systemie niż orzekanie o winie. Istotną kwestią jest poszukiwanie odpowiedzi na pytanie „jak to się stało”, a nie „kto zawinił”. Elastyczność systemu może być znacznie skuteczniej wzmocniona poprzez usunięcie braków systemowych niż poprzez usuwanie „niepasujących” jednostek.

e) **Dzielenie się wiedzą o bezpieczeństwie i doświadczeniami** poprzez aktywną wymianę informacji. Inny znany aforyzm wymownie ilustruje potrzebę dzielenia się danymi i wymianą informacji: „ucz się na błędach innych, nie będziesz żył wystarczająco długo, by sam je wszystkie popełnić”. Wspaniała tradycja branży lotniczej dzielenia się danymi musi zostać podtrzymana i, jeśli to w ogóle możliwe, wzmocniona.

f) **Integracja szkoleń bezpieczeństwa dla personelu operacyjnego.** Rzadko kiedy programy szkoleniowe dla personelu operacyjnego zawierają osobne części dotyczące bezpieczeństwa. Istnieje założenie, że odkąd „bezpieczeństwo jest odpowiedzialnością wszystkich" personel operacyjny jest ekspertem sam w sobie. Błąd tego typu rozumowania jest oczywisty i zostanie omówiony w rozdziale 7. Istnieje paląca potrzeba włączenia osobnych szkoleń zawierających podstawy zarządzania bezpieczeństwem na wszystkich poziomach szkoleń dla personelu operacyjnego.

g) **Skuteczne wdrażanie standardowych procedur działań (ang. SOPs)**, włączając w to użycie list czynności kontrolnych załogi oraz odprawy. Standardowe procedury działania (ang. SOPs), listy czynności kontrolnych załogi oraz odprawy, czy to na pokładzie statku powietrznego, czy w dziale kontroli ruchu lotniczego, czy w dziale obsługi, czy też na płycie lotniska są jednymi z najskuteczniejszych mechanizmów bezpieczeństwa, które personel operacyjny musi spełnić jako swoje codzienne obowiązki. To upoważnienie organizacji do przeprowadzania operacji zgodnie z wolą wyższego zarządu. Nie powinno się bagatelizować realnej wartości, poprawnie napisanych i wciąż dostosowywanych do standartowych procedur działania (SOPs) list czynności kontrolnych oraz odpraw.

h) **Ciągłe doskonalenie ogólnego poziomu bezpieczeństwa.** Zarządzanie bezpieczeństwem nie jest sprawą jednego dnia. To wciąż trwająca działalność, która może być udana tylko poprzez ciągłe doskonalenie.

3.7.2 Rezultatem wdrożenia tych ośmiu części składowych będzie odpowiedni poziom organizacyjny, który sprzyja bezpiecznym praktykom, zachęca do skutecznej komunikacji w zakresie bezpieczeństwa oraz aktywnie zarządza bezpieczeństwem.

### 3.8 CZTERY OBOWIĄZKI W ZARZĄDZANIU BEZPIECZEŃSTWEM

3.8.1 Obowiązki związane z zarządzaniem bezpieczeństwem mogą być podzielone na cztery ogólne i podstawowe sfery, takie jak:

a) **Określenie taktyk i procedur dotyczących bezpieczeństwa.** Taktyki postępowania i procedury są odzwierciedleniem tego, w jaki sposób zarząd życzy sobie przeprowadzania operacji lotniczych. Jasne określenie taktyk i procedur jest zatem podstawą, by personel operacyjny miał jasne wskazówki dotyczące zachowań operacyjnych, których organizacja oczekuje od personelu operacyjnego podczas codziennych działań.

b) **Przydzielanie środków finansowych na czynności związane z zarządzaniem bezpieczeństwem.** Zarządzanie bezpieczeństwem wymaga środków finansowych. Ich przydzielanie leży w gestii kierownictwa. Zarząd ma władzę, a zatem jest odpowiedzialny za przydzielanie środków finansowych służących łagodzeniu ryzyka jako konsekwencji zagrożeń, które osłabiają możliwości organizacji.

c) **Zaadaptowanie najlepszych praktyk branżowych.** Tradycja lotnictwa dotycząca doskonałości w bezpieczeństwie doprowadziła do ciągłego rozwoju solidnych praktyk związanych z bezpieczeństwem. Lotnictwo ma w dodatku tradycję dotyczącą wymiany informacji o bezpieczeństwie zarówno poprzez kanały instytucjonalne jak i nieformalne. Te dwa pozytywne sposoby powinny być wzmacniane i używane do adaptowania najlepszych praktyk w branży.

d) **Włączanie przepisów regulujących bezpieczeństwo w lotnictwie cywilnym.** Istnieje możliwość powstania błędnego założenia, że zarządzanie bezpieczeństwem uczyni panujące przepisy zbytecznymi i niepotrzebnymi. Ten pogląd musi być wyraźnie odrzucony. Zawsze będzie istniała potrzeba stworzenia ram dla przepisów, które stanowiłyby fundament wysiłków związanych z zarządzaniem bezpieczeństwem. W istocie rozsądne zarządzanie bezpieczeństwem może zostać zbudowane tylko w oparciu o rozsądne przepisy.

3.8.2 Podsumowując, zarządzanie bezpieczeństwem:

a) dotyczy całej operacji;

b) koncentruje się na procesach, jasno rozróżniając procesy od następstw;

c) opiera się na danych;

d) wiąże się z ciągłym monitoringiem;

e) jest ściśle dokumentowane;

f) celuje w stopniowe doskonalenie, a nie w dramatyczne zmiany;

g) opiera się na strategicznym planowaniu w odróżnieniu od fragmentarycznych inicjatyw.

# Rozdział 4

# ZAGROŻENIA

## 4.1 CEL I ZAWARTOŚĆ

Ten rozdział prezentuje podstawy identyfikacji zagrożeń oraz analizę następujących tematów:

a) Zagrożenie i konsekwencje;

b) Pierwsza zasada – zrozumienie zagrożenia;

c) Druga zasada – identyfikacja zagrożenia;

d) Trzecia zasada – analiza zagrożenia;

e) Czwarta zasada – dokumentacja zagrożeń.

## 4.2 ZAGROŻENIA I KONSEKWENCJE

4.2.1 Identyfikacja zagrożenia oraz zarządzanie ryzykiem są podstawowymi procesami dotyczącymi zarządzania bezpieczeństwem. Nie są one ani nowe ani nie zostały rozwinięte, jako konsekwencja ostatnich zainteresowań zarządzaniem bezpieczeństwem, a w szczególności systemami zarządzania bezpieczeństwem. Identyfikacja zagrożenia i zarządzanie ryzykiem są niezmiennymi elementami, leżącymi u samych podstaw najistotniejszej idei systemu bezpieczeństwa. To obejmujące wszystko, oparte na technice podejście, które przyczyniło się do budowy systemu i które zostało stworzone ponad czterdzieści lat temu. Różnica pomiędzy systemem tradycyjnym a obecnym systemem zarządzania bezpieczeństwem jest taka, że ze względu na swoje techniczne podłoże system bezpieczeństwa czerpał głównie z technicznych aspektów i komponentów systemu, mających konsekwencje dla bezpieczeństwa, w pewnym stopniu na niekorzyść czynnika ludzkiego. Z drugiej strony zarządzanie bezpieczeństwem zbudowane jest na dogmacie bezpieczeństwa systemu (identyfikacji zagrożenia i zarządzaniu ryzykiem) i rozszerza swoje pole o perspektywę włączenia czynników ludzkich oraz działania człowieka, jako kluczowych aspektów podczas budowania systemu i jego działania.

4.2.2 Rozróżnienie pomiędzy zagrożeniami a ryzykiem bezpieczeństwa jest często źródłem trudności i zamieszania. W celu kształtowania praktyk związanych z zarządzaniem bezpieczeństwem, które są właściwe i skuteczne, ważne jest zrozumienie czym jest zagrożenie a czym zagrożenie bezpieczeństwa. Ten rozdział omawia wyłącznie zagrożenia, podczas gdy rozdział 5 omawia zagrożenia bezpieczeństwa. Przy omawianiu zagrożeń, a także by pomóc w zrozumieniu różnicy pomiędzy zagrożeniami a ryzykiem bezpieczeństwa, dyskusja dzieli ogólne pojęcie zagrożenia na dwa składniki: zagrożenie samo w sobie oraz jego konsekwencje. Jasne zrozumienie różnicy pomiędzy tymi dwoma składnikami ma również kapitalne znaczenie dla praktyk związanych z zarządzaniem bezpieczeństwem.

4.2.3 Zagrożenie jest zdefiniowane jako stan lub przedmiot z potencjałem możliwości spowodowania urazów personelu, uszkodzeń sprzętu lub konstrukcji, utraty substancji lub zmniejszenie możliwości wypełnienia pierwotnych założeń. Systemy, w których ludzie muszą aktywnie i precyzyjnie posługiwać się technologią by osiągnąć cele gospodarcze poprzez świadczenie usług są znane jako systemy socjotechniczne. Wszystkie organizacje lotnicze są zatem systemami socjotechnicznymi. Zagrożenia są normalnym składnikiem systemów socjotechnicznych. Są integralne w kontekście, w którym ma miejsce świadczenie usług przez socjotechniczne systemy produkcji. Same w sobie zagrożenia nie są „złą rzeczą”. Zagrożenia nie koniecznie są niszczącym lub negatywnym składnikiem systemu. Tylko wtedy, kiedy zagrożenia wchodzą w sprzężenie z operacjami w systemie skierowanym na świadczenie usług, ich niszczący potencjał może stać się problemem dla bezpieczeństwa.

4.2.4 Weźmy pod uwagę na przykład wiatr, zwykły składnik środowiska naturalnego. Wiatr jest zagrożeniem: jest okolicznością o potencjale spowodowania urazów personelu, uszkodzeń sprzętu i konstrukcji, utratę substancji lub zmniejszenie możliwości wypełnienia pierwotnych założeń. Wiatr o sile piętnastu węzłów sam w sobie nie musi koniecznie nieść możliwości zniszczeń podczas operacji lotniczych. W istocie piętnastowęzłowy wiatr wiejący wzdłuż osi pasa startowego przyczyni się do polepszenia możliwości operacyjnych statku powietrznego podczas startu. Jednakże kiedy piętnastowęzłowy wiatr wieje pod kątem 90 stopni do osi pasa startowego staje się wiatrem bocznym. Wtedy zagrożenie sprzęga się z operacjami systemu (start i lądowanie statku powietrznego) nakierowanymi na świadczenie usług (potrzeba przetransportowania pasażerów lub ładunku do/z konkretnego lotniska zgodnie z harmonogramem) i niszczący potencjał zagrożenia staje się sprawą bezpieczeństwa (wypadnięcie z pasa startowego, ponieważ pilot może nie być w stanie sterować statkiem powietrznym ze względu na boczny wiatr). Ten przykład zilustrowany został w paragrafie 4.2.3: zagrożenie niekoniecznie musi być uważane za „czynnik negatywny" mający negatywne skutki. Zagrożenie jest integralną częścią kontekstu operacyjnego, a jego konsekwencjami można się zajmować poprzez różne strategie łagodzenia, które mogą powstrzymać jego niszczący potencjał, co zostanie omówione w dalszej części tego podręcznika.

4.2.5 Zagrożenie może nieść ze sobą negatywne konsekwencje. Niszczący potencjał, jaki niesie ze sobą zagrożenie urzeczywistnia się w jednej lub wielu jego konsekwencjach. W przytoczonym wyżej przykładzie dotyczącym wiatrów bocznych, jedną z konsekwencji zagrożenia „wiatrów bocznych" mogła być „utrata sterowania poprzecznego". Dalszą, poważniejszą konsekwencją mogło być „uszkodzenie podwozia statku powietrznego". Ważne jest zatem opisywanie wszystkich możliwych konsekwencji zagrożenia podczas jego analizy, a nie tylko tych najbardziej oczywistych i aktualnych.

4.2.6 Przy omawianiu konsekwencji zagrożeń należy mieć na uwadze dwie ważne kwestie. Pierwsza – zagrożenia należą do teraźniejszości. Są w większości przypadków częścią kontekstu operacyjnego i dlatego są obecne w miejscu pracy, zanim personel operacyjny „pojawi się w pracy". Zagrożenia są i powinny być wykrywalne podczas audytów, jako fizyczny składnik kontekstu operacyjnego lub miejsca pracy. Z drugiej strony konsekwencje zagrożenia należą do przyszłości. Nie ujawniają się dopóki zagrożenia nie wejdą w interakcję z określonymi operacjami systemu skierowanego na świadczenie usług. To w konsekwencji tej interakcji zagrożenia mogą ujawnić swój niszczący potencjał. Prowadzi to do bardzo ważnej zasady w zarządzaniu bezpieczeństwem: strategie łagodzenia powinny zmierzać ku prewencyjnemu powstrzymywaniu niszczącego potencjału zagrożeń, a nie oczekiwaniu aż konsekwencje zagrożeń ujawnią się i reaktywnemu zajmowaniu się jego konsekwencjami po fakcie.

4.2.7 Kwestia druga – dla celów zarządzania bezpieczeństwem konsekwencje zagrożeń powinny być opisywane w kategoriach operacyjnych. Wiele zagrożeń niesie w sobie możliwość ostatecznej i najbardziej ekstremalnej konsekwencji: utraty ludzkiego życia. Większość zagrożeń niesie możliwość utraty mienia, zniszczeń ekologicznych i podobnych konsekwencji wysokiego stopnia. Jednakże opisywanie konsekwencji zagrożeń w kategoriach ekstremalnych czyni trudnym zbudowanie strategii łagodzących, poza odwołaniem operacji. W celu budowania strategii łagodzących, obejmujących problemy związane z operacyjnymi konsekwencjami zagrożenia poniżej ekstremalnego (na przykład wiatry boczne), takie konsekwencje muszą być opisywane w kategoriach operacyjnych (wypadnięcie z pasa startowego), raczej niż w kategoriach ekstremalnych (utrata życia).

4.2.8 W rozdziale 2 omówiono bezpieczeństwo jako stan kontrolowanego zagrożenia. Opis konsekwencji zagrożeń, które mogą dotknąć konkretną operację jest częścią oceny zagrożeń bezpieczeństwa, jako konsekwencji zagrożeń (omawiane w rozdziale 5). Ocena ryzyka bezpieczeństwa, jako konsekwencji zagrożeń pozwala organizacji podjąć uzasadnioną decyzję dotyczącą tego, czy może ona osiągnąć stan kontroli ryzyka bezpieczeństwa i w ten sposób kontynuować operację. Jeśli następstwa zagrożenia (wiatry boczne) są opisane raczej w kategoriach ekstremalnych (utrata życia) niż w kategoriach operacyjnych (wypadnięcie z pasa startowego), ocena ryzyka bezpieczeństwa jest w dużym stopniu unieważniona, gdyż stan kontroli ryzyka bezpieczeństwa nie zostanie osiągnięty o ile nie zostaną poniesione ogromne wydatki, a prawdopodobnym złagodzeniem będzie odwołanie operacji.

### 4.3 PIERWSZA ZASADA – ZROZUMIENIE ZAGROŻEŃ

4.3.1 Jak już zostało omówione istnieje tendencja do mylenia zagrożeń z ich konsekwencjami. Jeśli ma to miejsce, wtedy opis zagrożenia w kategoriach operacyjnych raczej odzwierciedla konsekwencje niż zagrożenie samo w sobie. Innymi słowy opisywanie zagrożeń, jako ich konsekwencji nie należy do rzadkości.

4.3.2 Określenie i nazwanie zagrożenia, jako jego konsekwencji umożliwia nie tylko zatajanie prawdziwej natury i niszczącego potencjału rozpatrywanego zagrożenia, lecz także zakłóca identyfikację innych ważnych konsekwencji zagrożenia.

4.3.3 Z drugiej strony właściwe określenie i nazwanie zagrożeń pozwala dostrzec ich naturę i niszczący potencjał, właściwie wnioskować o źródłach i mechanizmach zagrożeń i, co najważniejsze, oceniać rezultaty (inne niż ekstremalne) w kategoriach rozmiaru potencjalnej straty, która jest jednym z ostatecznych skutków zarządzania ryzykiem, jak to omówione zostało w rozdziale 5.

4.3.4 Kolejny prezentowany przykład ilustruje różnice pomiędzy zagrożeniami a ich konsekwencjami. Lotnisko funkcjonuje z uszkodzoną sygnalizacją i oznakowaniem. To komplikuje cele nawigacji naziemnej użytkownikom lotniska, zarówno statkom powietrznym jak i pojazdom naziemnym. W takim przypadku właściwą nazwą dla zaistniałego zagrożenia mogło by być „nieczytelne oznakowanie lotniska" (to jest stan potencjalnego spowodowania urazów personelu, uszkodzenia wyposażenia i infrastruktury, utratę substancji lub zmniejszenie możliwości pełnienia zadanych funkcji). W wyniku takiego zagrożenia istnieje wiele możliwych następstw. Jednym z następstw (to jest jednym z potencjalnych rezultatów) zagrożenia „nieczytelnego oznakowania lotniska" może być wtargnięcie na pas startowy. Mogą też zaistnieć inne konsekwencje: pojazdy naziemne mogą wjechać do strefy zakazanej, statek powietrzny może kołować po niewłaściwej drodze do kołowania, mogą nastąpić kolizje statków powietrznych, kolizje pojazdów naziemnych, kolizje pomiędzy statkami powietrznymi i pojazdami naziemnymi i tak dalej. Stąd nazwanie zagrożenia, jako „wtargnięcie na pas startowy" zamiast „nieczytelnego oznakowania lotniska" maskuje naturę zagrożenia i zakłóca identyfikację innych ważnych konsekwencji. To prawdopodobnie prowadzi do częściowych lub niekompletnych strategii minimalizowania zagrożeń.

4.3.5 Zagrożenia mogą zostać podzielone na trzy główne grupy: zagrożenia naturalne, zagrożenia techniczne i zagrożenia ekonomiczne.

4.3.6 Zagrożenia naturalne są następstwem otoczenia, w którym mają miejsce operacje związane ze świadczeniem usług. Przykłady naturalnych zagrożeń to:

a) trudne warunki pogodowe lub zdarzenia klimatyczne (na przykład huragany, śnieżyce, susze, tornada, burze, pioruny i uskoki wiatru);

b) niekorzystne warunki atmosferyczne (na przykład zamarzające opady atmosferyczne, ulewne deszcze, śnieg, wiatr i ograniczenia widoczności);

c) zdarzenia geofizyczne (na przykład trzęsienia ziemi, erupcje wulkanów, tsunami, powodzie i obsunięcia ziemi);

d) warunki geograficzne (na przykład trudny teren lub rozległe powierzchnie wody);

e) zdarzenia w środowisku naturalnym (na przykład pożary, dzika przyroda oraz plagi insektów i zarazy); i/lub

f) zdarzenia z zakresu zdrowia publicznego (na przykład epidemie grypy i innych chorób).

4.3.7 Zagrożenia techniczne istnieją jako pochodna źródeł zasilania (elektryczność, paliwo, ciśnienie hydrauliczne, ciśnienie pneumatyczne i tak dalej) lub funkcji decydujących o bezpieczeństwie (możliwe awarie sprzętu, usterki w oprogramowaniu, ostrzeżenia i tak dalej) koniecznych przy operacjach związanych ze świadczeniem usług. Do przykładów zagrożeń technicznych zalicza się awarie:

a) statku powietrznego i jego składowych, systemów, podsystemów i pokrewnych urządzeń;

b) urządzeń, narzędzi i powiązanego wyposażenia; i/lub

c) urządzeń, systemów, podsystemów i pokrewnego sprzętu spoza organizacji.

4.3.8 Zagrożenia ekonomiczne są następstwem środowiska socjopolitycznego, w ramach którego mają miejsce operacje związane ze świadczeniem usług. Przykłady zagrożeń ekonomicznych to:

a) wzrost gospodarczy;

b) recesja;

c) koszty materiałów i sprzętu.

4.3.9 Czynności związane z zarządzaniem bezpieczeństwem będą przede wszystkim, lecz nie tylko nakierowane na problemy zagrożeń technicznych i naturalnych.

### 4.4 DRUGA ZASADA – IDENTYFIKACJA ZAGROŻENIA

4.4.1 Zostało omówione, że zagrożenia są częścią każdego produkcyjnego systemu socjotechnicznego. Stąd zakres zagrożeń w lotnictwie jest szeroki. Przykłady rozmiaru czynników i procesów, które powinno się rozpatrzyć przy zajmowaniu się identyfikacją zagrożenia to:

a) czynniki budowy, włączając budowę sprzętu i określenie celów;

b) procedury i praktyki operacyjne, włączając w to dokumentację i listy kontrolne, oraz ich uprawomocnienie w aktualnych warunkach operacyjnych;

c) komunikacja, włączając w to środki, terminologię i język;

d) czynniki związane z personelem, takie jak polityka rekrutacji w firmie, szkolenia, wynagrodzenia i przydział środków finansowych;

e) czynniki organizacyjne, takie jak kompatybilność celów gospodarczych i bezpieczeństwa, przydział środków finansowych, działające naciski i korporacyjna kultura bezpieczeństwa;

f) czynniki związane ze środowiskiem pracy, takie jak hałas i drgania, temperatura, oświetlenie oraz dostępność sprzętu ochronnego i odzieży;

g) czynnik nadzoru, włączając w to zastosowalność i wykonalność przepisów; certyfikację sprzętu, personelu i procedur, oraz stosowność nadzoru;

h) ochrona, włączając w to takie czynniki jak dostarczanie odpowiednich systemów wykrywania i ostrzegania, żywotność sprzętu i odporność na uszkodzenia;

i) działanie człowieka, ograniczone poprzez warunki zdrowotne i ograniczenia fizyczne.

4.4.2 Jak zostało omówione w rozdziale 3 zagrożenia mogą zostać zidentyfikowane w następstwie zdarzeń (wypadków lub incydentów), lub też mogą zostać zidentyfikowane poprzez prewencyjne procesy nakierowane na identyfikację zagrożeń zanim przyspieszą zaistnienie tych zdarzeń. Istnieją różne źródła identyfikacji zagrożeń. Niektóre źródła znajdują się wewnątrz organizacji, podczas gdy inne są na zewnątrz.

4.4.3 Przykłady wewnętrznych źródeł identyfikacji zagrożeń dostępnych w organizacji:

a) analiza danych lotu;

b) dobrowolny system raportowania;

c) inspekcje bezpieczeństwa;

d) audyty bezpieczeństwa;

e) programy monitorowania operacji;

f) analiza trendów;

g) informacje zwrotne ze szkoleń;

h) badania incydentów i wynikające z nich wnioski.

4.4.4 Przykłady zewnętrznych źródeł identyfikacji zagrożeń dostępnych w organizacji:

a) raporty o wypadkach;

b) państwowy obowiązkowy system raportowania o wypadkach;

c) państwowy dobrowolny system raportowania;

d) państwowe audyty nadzorcze;

e) systemy wymiany informacji.

4.4.5 Podstawową omawianą tu kwestią jest to, że żadne źródła lub program nie zastąpi całkowicie innych, lub też nie uczyni innych źródeł i programów zbytecznymi i niepotrzebnymi. Identyfikacja zagrożenia prowadzona przez sprawdzone praktyki zarządzania bezpieczeństwem polega na rozważnym łączeniu wewnętrznych i zewnętrznych źródeł, procesów reaktywnych, prewencyjnych i prognozowania oraz programów, które leżą u ich podstaw.

4.4.6 Cały personel organizacji lotniczych powinien być przeszkolony w zakresie zarządzania bezpieczeństwem na poziomie proporcjonalnym do jego obowiązków, tak, że każdy pracownik organizacji jest przygotowany i zdolny do identyfikacji zagrożenia i informowania o nim. Z tego punktu widzenia identyfikacja zagrożenia i informowanie o nim jest obowiązkiem każdego. Zajmowałby się tym zwykle personel przydzielony do biura/wydziału bezpieczeństwa, omówionego w rozdziale 8. Stąd, wychodząc poza poprzedni zakres, identyfikacja zagrożenia w organizacjach lotniczych jest obowiązkiem każdego pracownika, lecz odpowiedzialność za jego identyfikację leży po stronie wyznaczonego do tego personelu.

4.4.7 Sposób identyfikacji zagrożeń będzie zależeć od źródeł i ograniczeń każdej organizacji. Niektóre organizacje uruchomią wszechstronne, oparte na technologii, programy identyfikacji zagrożenia. Inne organizacje uruchomią skromne programy identyfikacji zagrożenia, bardziej odpowiadające ich rozmiarom oraz skomplikowaniu przeprowadzanych przez nie operacji. Mimo to identyfikacja zagrożenia, bez względu na realizację programów, skomplikowanie operacji i rozmiary organizacji, musi być procesem formalnym, jasno opisanym w dokumentacji dotyczącej bezpieczeństwa w organizacji. Identyfikacja zagrożenia ad hoc jest niedopuszczalną praktyką w zarządzaniu bezpieczeństwem.

4.4.8 Przy rozwiniętych praktykach zarządzania bezpieczeństwem identyfikacja zagrożenia jest ciągle trwającą, codzienną czynnością, która nie ustaje ani nie ma przerw. Jest integralną częścią procesu organizacyjnego, nakierowanego na świadczenie usług, które oferuje organizacja. Niemniej jednak istnieją trzy określone warunki, które nakazują poświęcenie specjalnej uwagi kwestii identyfikacji zagrożenia. Te trzy warunki powinny wywołać bardziej wnikliwe i dalekosiężne działania związane z identyfikacją zagrożenia. Są to:

a) sytuacje, w których organizacja doświadcza niewyjaśnionego zwiększania się liczby zdarzeń na tle bezpieczeństwa lub naruszeń przepisów;

b) sytuacje, w których przewiduje się poważne zmiany operacyjne, włącznie z wymianą podstawowego personelu, sprzętu lub systemów;

c) przed i podczas zmian organizacyjnych, włączając w to szybki wzrost lub kurczenie się organizacji, fuzje, przejęcia lub redukcje.

### 4.5 TRZECIA ZASADA – ANALIZA ZAGROŻENIA

4.5.1 Identyfikacja zagrożenia jest niepotrzebnym zadaniem jeżeli nie czerpie się informacji o bezpieczeństwie z zebranych danych. Pierwszym krokiem przy gromadzeniu informacji o bezpieczeństwie jest analiza zagrożenia.

4.5.2 Analiza zagrożenia jest w istocie procesem trzystopniowym:

a) **Krok pierwszy.** Określ zagrożenie ogólne (znane również jako zagrożenie najwyższego stopnia [ang. TLH]). Zagrożenie ogólne w kontekście tego podręcznika jest używane jako termin, który ma za zadanie skoncentrowanie się na kwestiach bezpieczeństwa, jak również pomoc w upraszczaniu śledzenia i klasyfikacji wielu pojedynczych zagrożeń wypływających z zagrożenia ogólnego.

b) **Krok drugi.** Podziel zagrożenie ogólne na zagrożenia pojedyncze lub składowe zagrożenia ogólnego. Każde określone zagrożenie będzie prawdopodobnie miało zróżnicowany i unikalny zestaw czynników doraźnych, przez co każde pojedyncze zagrożenie staje się odmienne i unikalne ze swej natury.

c) **Krok trzeci.** Połącz dane konkretne zagrożenia z potencjalnymi określonymi konsekwencjami, to jest określonymi zdarzeniami i skutkami.

4.5.3 Oto przykład służący zilustrowaniu pojęć takich jak zagrożenie ogólne, konkretne zagrożenie oraz konsekwencje. Międzynarodowe lotnisko, które obsługuje 100 000 operacji rocznie uruchamia projekt powiększenia oraz ułożenia nowej nawierzchni jednego z dwóch krzyżujących się pasów startowych. W takim wypadku powinno się zastosować następujący trzystopniowy proces analizy zagrożenia:

a) **Krok A.** Ustal zagrożenie ogólne (powiadomienie o ryzyku lub ryzyku najwyższego stopnia [ang. TLH])

– budowa na lotnisku;

b) **Krok B.** Zidentyfikuj pojedyncze zagrożenia lub składowe zagrożenia ogólnego

– sprzęt budowlany;

– zamknięte drogi kołowania itd.

c) **Krok C.** Połącz konkretne zagrożenia z określonymi skutkami

– statek powietrzny wchodzący w kolizję ze sprzętem budowlanym (sprzęt budowlany)

– statek powietrzny startujący ze złego pasa (zamknięte drogi kołowania), itd.

4.5.4 Przykład budowy pasa startowego omówiony w paragrafie 4.5.3 może służyć do poszerzenia dyskusji na temat „dylematu dwóch P” w rozdziale 3 o analizę zagrożenia: wydajne i bezpieczne świadczenie usług wymaga ciągłego równoważenia celów gospodarczych i celów bezpieczeństwa. W przykładzie z budową pasa startowego istnieje jasno określony cel (ekonomiczny): utrzymanie regularnych operacji lotniska podczas realizacji projektu przebudowy pasa startowego. Istnieje też podobnie jasny cel bezpieczeństwa (ochrony): podtrzymanie istniejących marginesów bezpieczeństwa operacji lotniczych podczas przebudowy pasa startowego. Przy analizie zagrożenia na pierwszym planie kalkulacji muszą się znaleźć dwie podstawowe przesłanki zarządzania bezpieczeństwem:

a) zagrożenie jest potencjalnym słabym punktem, nieodłącznym od socjotechnicznych systemów produkcji. Analizy zagrożenia są konieczną częścią systemu jako wynik możliwości, jakich dostarczają lub mogą potencjalnie przynieść systemowi przy świadczeniu usług. Miejsca pracy w lotnictwie niosą w sobie zagrożenia, zajmowanie się którymi może być kosztowne, ale operacje muszą być kontynuowane;

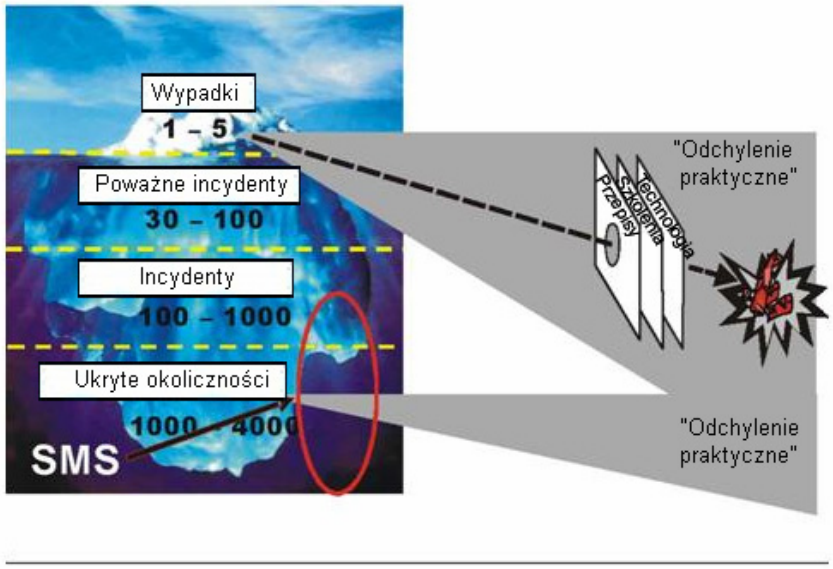
b) identyfikacja zagrożenia jest zmarnowanym wysiłkiem, jeśli ograniczy się ją tylko do badania skutków rzadkich wypadków, w których nastąpiły poważne urazy i szkody. Przedstawione zostało to na ilustracji 4-1, poprzez połączenie identyfikacji zagrożenia z „odchyleniem praktycznym”, omówionym w rozdziale 3.

## 4.6 CZWARTA ZASADA – DOKUMENTACJA ZAGROŻEŃ

4.6.1 Zagrożenia zazwyczaj utrwalają się w systemie i przynoszą swój niszczący potencjał głównie poprzez nieobecność lub nieskuteczność jego identyfikacji. Brak identyfikacji zagrożenia często jest rezultatem:

a) braku myślenia o warunkach operacyjnych, które mogą uwolnić niszczący potencjał zagrożeń;

b) niewiedzy o warunkach operacyjnych, która może uwolnić niszczący potencjał zagroże;




**Ilustracja 4 - 1. Szczegóły identyfikacji ryzyka**

c) niechęci wzięcia pod uwagę lub zbadania warunków operacyjnych, które mają możliwość uwolnienia niszczącego potencjału zagrożeń;

d) niechęci do przeznaczania pieniędzy na badanie warunków operacyjnych, które dają możliwość uwolnienia niszczącego potencjału zagrożeń.

4.6.2 Nieświadomość lub niechęć może być przezwyciężona tylko poprzez posiadanie stosownej wiedzy. Formalne dokumentowanie zagrożeń jest zatem istotnym wymogiem dla celów identyfikacji zagrożenia, jak również potwierdzeniem rozwiniętego zarządzania bezpieczeństwem. Informacje dotyczące bezpieczeństwa (czyli zanalizowane nieprzetworzone dane) oraz rozpoznanie bezpieczeństwa (to jest informacje o bezpieczeństwie, które zostały potwierdzone, a następnie zanalizowane poprzez dodanie kontekstu) są połączone w celu wygenerowania wiedzy na temat bezpieczeństwa, która musi formalnie znaleźć się w organizacji, a nie w świadomości pojedynczych jej członków. Formalne przechowywanie wiedzy na temat bezpieczeństwa pomoże oprzeć decyzje dotyczące bezpieczeństwa na faktach, a nie na opiniach.

4.6.3 Stosowne zarządzanie dokumentacją dotyczącą identyfikacji zagrożenia jest ważne jako procedura formalna w celu przekładania surowych informacji operacyjnych dotyczących bezpieczeństwa w wiedzę na temat zagrożenia. Ciągłe opracowywanie oraz formalne zarządzanie wiedzą na temat zagrożenia staje się „archiwum bezpieczeństwa" organizacji. W celu rozwijania wiedzy o ryzyku, a następnie budowania „archiwum bezpieczeństwa" należy pamiętać, że śledzenie i analizowanie zagrożenia jest ułatwione poprzez standaryzację:

a) używanych definicji i terminów;

b) rozumienia używanych terminów;

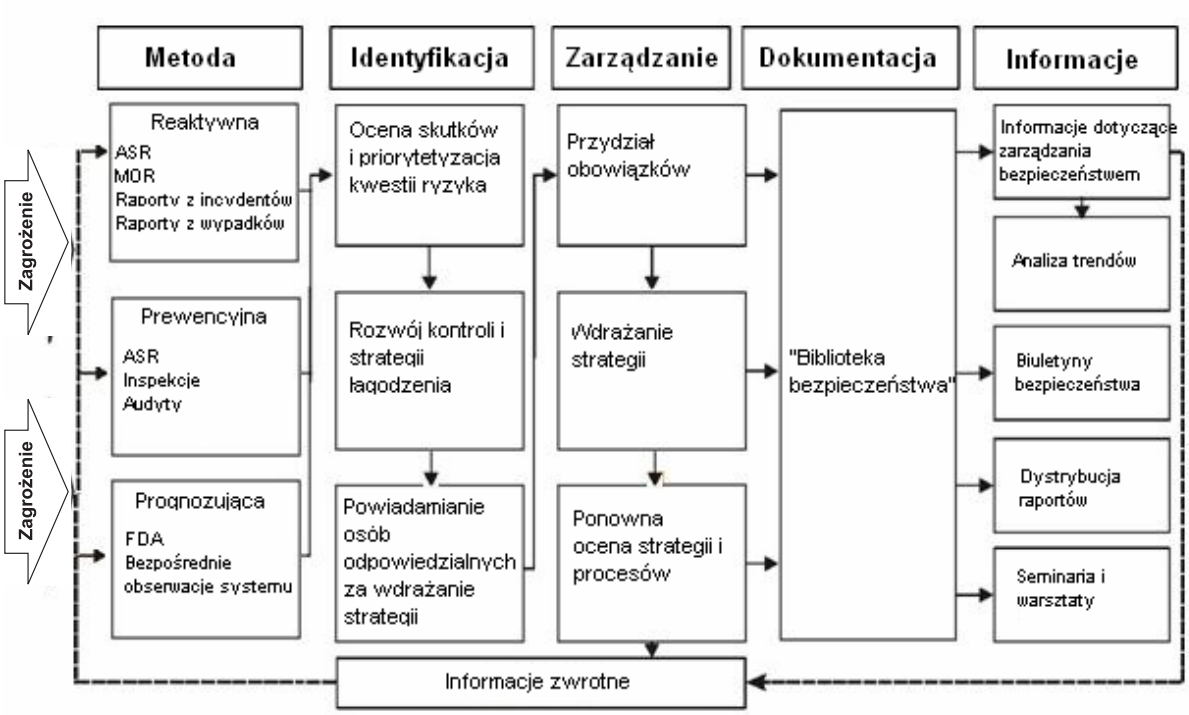
c) zatwierdzania zebranych informacji o bezpieczeństwie;

d) raportowania (tego, czego organizacja oczekuje);

e) pomiaru zebranych informacji;

f) zarządzania zebranymi informacjami.

4.6.7 Ilustracja 4-2 pokazuje proces dokumentowania zagrożenia. Zagrożenia są stale dokumentowane poprzez środki reaktywne, prewencję i prognozowanie oraz podstawowe metody zbierania informacji dotyczących bezpieczeństwa. Po zebraniu danych i identyfikacji zagrożenia, informacje dotyczące zagrożenia są oceniane w kategoriach skutków oraz priorytetów i obowiązków związanych z reakcją i strategią łagodzenia zagrożenia. Wszystkie informacje, włączając w to zagrożenie, skutki, priorytety, obowiązki i strategie muszą zostać zgromadzone w „archiwum bezpieczeństwa" organizacji. Stworzenie „biblioteki bezpieczeństwa" to nie tylko zabezpieczenie korporacyjnej pamięci w zakresie bezpieczeństwa, ale również takie „archiwum" staje się źródłem wiedzy na temat bezpieczeństwa, która może zostać użyta jako punkt odniesienia podczas podejmowania przez organizacje decyzji dotyczących bezpieczeństwa. Wiedza na temat bezpieczeństwa zawarta w „archiwum bezpieczeństwa" przynosi informacje zwrotne oraz weryfikację, dzięki której można mierzyć i analizować zagrożenie oraz zarządzać jego skutkami, jak również oceniać skuteczność źródeł i metod zbierania informacji na temat bezpieczeństwa. Wiedza ta dostarcza również materiału do analizy trendu, a także służy do celów edukacyjnych (biuletyny, raporty, seminaria i tym podobne).




Ilustracja 4-2. Dokumentowanie zagrożeń

## Dodatek 1 do Rozdziału 4

# ANALIZA INFORMACJI

1. Po zebraniu oraz zapisaniu informacji dotyczących bezpieczeństwa pochodzących z różnych źródeł identyfikacji ryzyka, znaczące wnioski mogą zostać wyciągnięte tylko poprzez analizę tych informacji. Zredukowanie tych informacji do prostych statystyk nie jest użyteczne jeśli nie dokona się oceny ich praktycznego znaczenia w celu określenia problemu, który może zostać rozwiązany.

2. Zakładając bazy danych dotyczące bezpieczeństwa oraz systemów raportowania, organizacje powinny analizować informacje zawarte w raportach oraz bazach danych w celu podejmowania wszelkich wymaganych czynności.

### CO TO JEST ANALIZA INFORMACJI?

3. Analiza informacji jest procesem gromadzenia faktów przy użyciu określonych metod, narzędzi i technik. Poza tym może być stosowana jako:

a) pomoc przy decydowaniu o dodatkowych potrzebnych informacjach;

b) pomoc przy ustalaniu podstawowych czynników w razie deficytu bezpieczeństwa;

c) pomoc przy dochodzeniu do wiążących wniosków.

4. Analiza jest oparta o faktyczne informacje pochodzące z różnych źródeł. Właściwe dane muszą zostać zebrane, uporządkowane i przechowywane. Metody analityczne oraz narzędzia potrzebne do analizy są następnie wybierane i zastosowane. Analiza bezpieczeństwa jest często wielokrotna, wymaga wielu cykli. Może być jakościowa i ilościowa. Brak podstawowych danych ilościowych może wymusić poleganie w większym stopniu na jakościowych metodach analizy.

### OBIEKTYWIZM I UKIERUNKOWANIE

5. Należy brać pod rozwagę wszystkie istotne informacje, jednakże nie wszystkie są rzetelne. Ograniczenia czasowe nie zawsze pozwalają na zgromadzenie i ocenę wystarczającej liczby informacji zapewniających obiektywizm. Czasami można wnioskować na podstawie intuicji. Nie są to wnioski zgodne z obiektywizmem wymaganym przy wiarygodnej analizie bezpieczeństwa.

6. Do pewnego stopnia ludzie są podatni na wstępne ukierunkowanie przy ocenianiu. Dotychczasowe doświadczenie będzie często wpływało na osąd, jak również kreatywność przy ustalaniu hipotez. Jedna z najczęstszych form błędu w ocenie jest znana jako „potwierdzenie ukierunkowania”. Jest to tendencja do szukania i wybierania informacji, które potwierdzają to, co już jest uważane przez oceniającego za prawdziwe.

### METODY I NARZĘDZIA ANALIZY

7. Do analizy bezpieczeństwa stosowane są różne metody. Niektóre z nich są zautomatyzowane, a niektóre nie. W dodatku istnieje kilka narzędzi analizy opartych na oprogramowaniu (wymagające różnych poziomów umiejętności do skutecznego ich stosowania). Poniżej znajduje się lista niektórych analitycznych metod i narzędzi, które są dostępne:

a) **Analiza statystyczna.** Wiele analitycznych metod i narzędzi używanych w analizie bezpieczeństwa jest opartych na procedurach i pojęciach statystycznych; na przykład analiza ryzyka używa pojęć statystycznego prawdopodobieństwa. Statystyka gra główną rolę w analizie bezpieczeństwa poprzez pomoc w szacowaniu sytuacji, tym samym dając pojęcie o sytuacji poprzez liczby. Metoda ta przynosi bardziej wiarygodne rezultaty i przekonywujące argumenty na rzecz bezpieczeństwa.

Typ analizy przeprowadzanej na poziomie działań zarządzania bezpieczeństwem przez organizację wymaga podstawowych umiejętności analizowania danych numerycznych, identyfikowania trendów, dokonywania podstawowych obliczeń statystycznych, takich jak średnie arytmetyczne, centyle i mediana. Metody statystyczne są również użyteczne przy graficznych prezentacjach analiz.

Przy operowaniu dużymi ilościami danych zaleca się stosowanie komputerów. Większość analiz i procedur statystycznych jest dostępna w pakietach oprogramowania do celów komercyjnych (na przykład Microsoft Excel). Używając takich aplikacji dane mogą być wprowadzane bezpośrednio do wstępnie przygotowanej procedury. Mimo, że szczegółowe rozumienie teorii statystycznej stojącej za techniką nie jest wymagane, to jednak analityk powinien rozumieć jak dana procedura działa i jakie zakładane rezultaty ma przynosić.

Jakkolwiek statystyka jest potężnym narzędziem przy analizie bezpieczeństwa może być także używana w niewłaściwy sposób, prowadząc w konsekwencji do błędnych wniosków. Należy zachować ostrożność przy doborze i użyciu danych w analizie statystycznej. W celu zapewnienia właściwego zastosowania bardziej skomplikowanych metod może być potrzebne wsparcie specjalistów od analizy statystycznej.

b) **Analiza trendu.** Poprzez monitorowanie trendów w danych dotyczących bezpieczeństwa można przewidywać przyszłe wydarzenia. Pojawiające się trendy mogą wskazywać na zalążek ryzyka. Metod statystycznych używa się do oceny ważności zauważonych trendów. Określa się wówczas wyższe i niższe limity akceptowalnego działania w porównaniu do bieżących działań. Analiza trendu służy wtedy do „wszczęcia” alarmu, gdy działanie znajduje się na granicy akceptowalnych limitów.

c) **Porównania normatywne.** Ilość danych może nie być wystarczająca, by zapewnić rzeczową podstawę porównania, w odniesieniu do której zestawia się okoliczności wydarzenia lub sytuacji poddanej badaniu w codziennym doświadczeniu. Brak wiarygodnych danych normatywnych często stawia pod znakiem zapytania użyteczność analiz bezpieczeństwa. W takich wypadkach może być konieczne pobieranie próbek z doświadczenia w realnym świecie w podobnych warunkach pracy. Zwykłe programy monitorujące operacje dostarczają użytecznych danych normatywnych do analizy operacji lotniczych.

d) **Symulacje i testy.** W niektórych przypadkach ryzyko może stać się widoczne poprzez testy; na przykład do analizowania defektów materiałowych wymagane są testy laboratoryjne. Przy budzącej wątpliwości procedurze operacyjnej może być nakazana symulacja w terenie w rzeczywistych warunkach pracy lub w symulatorze.

e) **Panel ekspertów.** Biorąc pod uwagę zróżnicowaną naturę ryzyka oraz różne możliwe perspektywy oceny poszczególnych niebezpiecznych okoliczności, należy zasięgać opinii innych, w tym pracowników i specjalistów. Multidyscyplinarny zespół powołany do oceny oznak niebezpiecznych okoliczności może również brać udział w określeniu i oszacowaniu najlepszego możliwego przebiegu czynności naprawczych.

f) **Analiza kosztów i korzyści.** Akceptacja zalecanych wytycznych kontroli bezpieczeństwa może być zależna od wiarygodnej analizy kosztów i korzyści. Koszt wdrożenia proponowanych zaleceń jest mierzony w stosunku do zakładanych korzyści w czasie. Niekiedy analiza kosztów i korzyści może sugerować, że preferowana jest akceptacja konsekwencji ryzyka niż czas, wysiłek i koszty konieczne do wdrożenia czynności naprawczych.

– – – – – – – – – – – – –

## Dodatek 2 do Rozdziału 4

# ZARZĄDZANIE INFORMACJAMI DOTYCZĄCYMI BEZPIECZEŃSTWA

### 1. UWAGI OGÓLNE

1.1 Niezbędnym składnikiem zarządzania bezpieczeństwem są dobrej jakości dane. Skuteczne zarządzanie bezpieczeństwem w pełni zależy od danych. Informacje zebrane z raportów operacyjnych i serwisowych, raportów bezpieczeństwa, audytów, ocen praktyk pracy, itd. generują wiele danych – chociaż nie wszystkie z nich są istotne dla zarządzania bezpieczeństwem. Zbiera się i przechowuje tak liczne dane związane z bezpieczeństwem, że istnieje ryzyko przytłoczenia nimi menedżerów, przez co użyteczność tych danych wymaga kompromisowych rozwiązań. Solidne zarządzanie bazami danych organizacji stanowi podstawę skutecznych funkcji zarządzania bezpieczeństwem (takich jak monitorowanie trendu, szacowanie ryzyka, analizy kosztów i korzyści oraz badania wypadków).

1.2 Argument za zmianami w bezpieczeństwie musi być oparty na analizie zgromadzonych danych dotyczących bezpieczeństwa. Zbudowanie i utrzymanie bazy danych z zakresu bezpieczeństwa dostarcza istotnego narzędzia dla zarządzających korporacją, zarządzających bezpieczeństwem oraz dla organów monitorujących system bezpieczeństwa. Niestety wielu bazom danych brakuje jakości potrzebnej do tego, by dostarczyć pewnych podstaw do ustanowienia hierarchii ważności bezpieczeństwa, oszacowania skuteczności środków łagodzenia ryzyka oraz inicjowania badań związanych z bezpieczeństwem. Interpretacja danych, baz danych oraz użycie właściwych narzędzi wymagane jest przy podejmowaniu właściwych i uzasadnionych decyzji.

1.3 Coraz częściej używa się oprogramowania komputerowego, aby ułatwić zapisywanie, przechowywanie, analizę i prezentację informacji o bezpieczeństwie. Obecnie możliwe jest przeprowadzanie skomplikowanych analiz informacji z baz danych. Na rynku dostępny jest szeroki zakres relatywnie niedrogich elektronicznych baz danych do użytku komputerów biurowych, zdolnych do wspierania wymaganego przez organizację zarządzania danymi. Te niezależne systemy mają tę dobrą stronę, że nie korzystają z głównego systemu komputerowego organizacji, dzięki czemu poprawie ulega stan bezpieczeństwa danych.

### 2. WYMAGANIA DOTYCZĄCE SYSTEMU INFORMACJI

W zależności od wielkości organizacji użytkownicy potrzebują systemu o wielu możliwościach i odpowiedniej wydajności, w celu zarządzania danymi dotyczącymi bezpieczeństwa. Ogólnie rzecz biorąc użytkownicy potrzebują:

a) systemu z możliwością przetwarzania dużych ilości danych, dotyczących bezpieczeństwa, w użyteczne informacje, które będą wspierać proces podejmowania decyzji;

b) systemu, który zredukuje ilość pracy zarządu i personelu;

c) zautomatyzowanego systemu, który może zostać przystosowany do ich kultury pracy;

d) systemu, który może działać przy relatywnie niskich kosztach.

### 3. INTERPRETACJA BAZ DANYCH

3.1 Aby wykorzystać potencjalne możliwości, jakie dają bazy danych, potrzebne jest podstawowe rozumienie ich działania, czyli odpowiedź na pytanie: co to jest baza danych? Wszelkie informacje, które zostały zgrupowane w zorganizowany sposób mogą być uważane za bazę danych. Dokumentację papierową można utrzymywać według prostego systemu wypełniania (jest to ręcznie sterowana „baza danych”), lecz taki system wystarczy tylko w przypadku najmniejszych operacji. Magazynowanie, rejestrowanie, przywoływanie oraz odnajdywanie danych to skomplikowane przedsięwzięcia. Dane o bezpieczeństwie, z różnych źródeł, powinny być przechowywane w elektronicznej bazie danych, która ułatwia odnajdywanie informacji w różnych formatach.

3.2 Możliwość manipulowania, analizowania i odnajdywania informacji na różne sposoby znana jest jako zarządzanie bazą danych. Większość pakietów oprogramowania do zarządzania bazami danych włącza do definicji bazy danych następujące elementy organizacyjne:

a) **Zapis.** Grupowanie informacji, które pasują do siebie jako całość (takich jak wszystkie dane dotyczące jednego wypadku);

b) **Pole.** Każda oddzielna informacja w spisie (taka jak data lub miejsce wypadku);

c) **Plik.** Grupa dokumentów mających tę samą strukturę i związki (takich jak wszystkie wypadki na tle problemów z silnikiem w danym roku).

3.3 Bazy danych są uważane za „zbudowane" wtedy, kiedy każde pole danych ma ustaloną wielkość i kiedy ich format jest jasno zdefiniowany przez numer, datę, odpowiedź „tak/nie", charakter lub tekst. Dla danego użytkownika zazwyczaj dostępny jest tylko ustalony wybór wartości. Wartości te są przechowywane w plikach odsyłaczach, często nazywanych tabelami bazy lub tabelami z listą wartości, na przykład wybór marek statków powietrznych i modeli z ustalonej z góry listy. W celu umożliwienia analizy ilościowej oraz systematycznych poszukiwań tekstowe niesformatowane hasło w zbudowanych bazach danych jest zminimalizowane poprzez ograniczenie go do określonej wielkości pola. Często taka informacja jest kategoryzowana poprzez system słów kluczowych.

3.4 Bazy danych są uważane za „tekstowe" kiedy ich zasoby informacji są przede wszystkim dokumentami pisemnymi (na przykład podsumowania dotyczące wypadków i incydentów lub pisemna korespondencja). Dane są indeksowane i przechowywane w niesformatowanych polach tekstowych. Niektóre bazy danych zawierają ogromne ilości uporządkowanych danych tekstowych, jednakże nowoczesne bazy danych są czymś więcej niż tylko elektronicznymi sekretarzykami.

## 4. OGRANICZENIA BAZ DANYCH

Trzeba liczyć się z ograniczeniami podczas budowania, utrzymywania i używania baz danych. Niektóre z tych ograniczeń odnoszą się wprost do systemu bazy danych, podczas gdy inne dotyczą obchodzenia się z samymi danymi. Aby uniknąć błędnych wniosków i decyzji użytkownicy bazy danych powinni rozumieć jej ograniczenia. Użytkownicy bazy danych powinni także znać przeznaczenie, dla którego baza danych została stworzona oraz wiarygodność informacji wprowadzonych przez organizację, która ją zbudowała i utrzymuje.

## 5. INTEGRALNOŚĆ BAZY DANYCH

5.1 Bazy danych dotyczące bezpieczeństwa są strategiczną częścią działań związanych z zarządzaniem bezpieczeństwem w organizacji. Dane są z różnych stron narażone na deformację i należy dopilnować, aby chroniona była ich integralność. Dostęp do bazy danych może mieć wielu pracowników, którzy wprowadzają do niej informacje. Inni przy wypełnianiu swoich obowiązków związanych z bezpieczeństwem będą potrzebować dostępu do tych danych. Dostęp z wielu stron systemu sieciowego może zwiększyć podatność na zniszczenia bazy danych.

5.2 Użyteczność bazy danych jest narażona, gdy nie przykłada się wystarczającej uwagi do zabezpieczania danych. Bazę danych psują: braki w danych, opóźnienia we wprowadzaniu bieżących danych, nieścisłe wprowadzanie danych, itd. Nawet użycie najlepszych narzędzi analitycznych nie może zrekompensować błędnych danych.

## 6. ZARZĄDZANIE BAZĄ DANYCH

### Ochrona danych dotyczących bezpieczeństwa

Ze względu na możliwość złego użycia danych dotyczących bezpieczeństwa, które zostały zebrane tylko w celach zwiększania bezpieczeństwa lotniczego, zarządzanie bazą danych musi się zaczynać od ich zabezpieczenia. Zarządzający bazą danych muszą zrównoważyć potrzebę ochrony danych z jej udostępnieniem tym, którzy mogą zwiększyć bezpieczeństwo lotnicze. Ochrona danych dotyczących bezpieczeństwa zawiera:

a) adekwatność przepisów dotyczących dostępu do informacji w stosunku do wymagań zarządzania bezpieczeństwem;

b) politykę chronienia danych przez organizację;

c) uniemożliwienie identyfikacji poprzez usunięcie wszystkich szczegółów, które mogą zasugerować stronie trzeciej tożsamość osób (na przykład numery lotów, daty/godziny, miejsca i typy statków powietrznych);

d) systemy bezpieczeństwa informacji, przechowywania danych i sieci łączności;

e) ograniczenie dostępu do baz danych tylko dla tych, którzy „muszą wiedzieć”;

f) zakazy nieupoważnionego użycia danych.

## 7. MOŻLIWOŚCI BAZY DANYCH DOTYCZĄCYCH BEZPIECZEŃSTWA

Właściwości funkcjonalne i cechy różnych systemów zarządzania bazą danych różnią się i każda powinna być brana pod uwagę przed przyjęciem systemu najbardziej odpowiadającego potrzebom operatora. Doświadczenie pokazuje, że incydenty związane z bezpieczeństwem lotniczym są najlepiej utrwalane i śledzone przy użyciu bazy danych w komputerze osobistym. Liczba dostępnych funkcji zależy od wybranego typu systemu. Podstawowe funkcje powinny umożliwić użytkownikowi przeprowadzenie następujących zadań:

a) logowania wypadków w różnych kategoriach;

b) łączenia wydarzeń z powiązanymi z nimi dokumentami (na przykład raportami lub fotografiami);

c) monitorowania trendów;

d) opracowywania analiz, wykresów i raportów;

e) sprawdzania dokumentów historycznych;

f) dzielenia się danymi z innymi organizacjami;

g) monitorowania badania wypadków;

h) oznaczania odpowiedzi na zaległe działania.

## 8. ASPEKTY WYBORU BAZY DANYCH

8.1 Wybór dostępnych na rynku systemów baz danych będzie zależał od oczekiwań użytkownika, wymaganych danych, systemu operacyjnego komputera oraz stopnia skomplikowania zapytań, z którymi będzie musiał się zmierzyć. Dostępne są różnorodne programy o zróżnicowanych możliwościach i wymaganiach. Podjęcie decyzji o tym, który typ wybrać wymaga rozważenia takich względów jak:

a) **Przyjazność systemu dla użytkownika.** System powinien być intuicyjnie łatwy w użyciu. Niektóre programy oferują szeroki zakres możliwości, ale wymagają dużego przygotowania. Niestety często dochodzi do kompromisu pomiędzy przyjaznością systemu dla użytkownika a mocą wyszukiwania; im bardziej przyjazne użytkownikowi narzędzie, tym mniej prawdopodobne, że będzie ono w stanie poradzić sobie z bardziej skomplikowanym zapytaniem.

b) **Dostęp.** Chociaż dostęp do wszystkich szczegółów przechowywanych w bazie danych to stan idealny, nie wszyscy użytkownicy potrzebują tego w tak szerokim zakresie. Struktura i skomplikowanie bazy danych będzie wpływać na wybór konkretnego narzędzia wyszukiwania.

c) **Wydajność.** Miarą wydajności jest skuteczność działania systemu. Zależy ona od następujących czynników: 1) jak skutecznie dane są zdobywane, przechowywane i monitorowane; 2) czy dane są przechowywane w formacie, który umożliwia dostrzeżenie trendu lub przeprowadzanie innych analiz; 3) od skomplikowania struktury bazy danych; 4) budowy systemu (lub sieci) komputera głównego.

d) **Elastyczność.** Elastyczność zależy od zdolności systemu do: 1) przetwarzania różnorodnych zapytań; 2) filtrowania i sortowania danych; 3) użycia logiki binarnej (tj. czy system radzi sobie z warunkami „i/lub", takimi jak np. „wszyscy piloci, którzy są kapitanami i mają 15 000 godzin w powietrzu" lub „wszyscy piloci, którzy są kapitanami lub mają 15 000 godzin w powietrzu"; 4) przeprowadzania podstawowych analiz (obliczeń i tabeli); 5) wytwarzania danych określonych przez użytkownika; 6) łączenia się z innymi bazami danych w celu pobierania i eksportowania danych.

8.2 Koszty różnią się w zależności od wymagań organizacji. Cena wyznaczona przez niektórych sprzedawców systemu jest stała, co umożliwia wielu użytkownikom korzystanie z jednej licencji. Zdarzają się inni sprzedawcy systemów, którzy zwiększają ceny w zależności od liczby użytkowników. Nabywca powinien wziąć pod uwagę następujące czynniki wpływające na cenę:

a) koszty instalacji;

b) koszty szkolenia;

c) koszty unowocześniania oprogramowania;

d) koszty obsługi i utrzymania;

e) inne koszty oprogramowania licencyjnego, które mogą okazać się konieczne.

# Rozdział 5

# RYZYKO BEZPIECZEŃSTWA

## 5.1 CEL I ZAWARTOŚĆ

Rozdział ten opisuje podstawy zarządzania ryzykiem bezpieczeństwa. Rozdział składa się z następujących tematów:

a) Definicja ryzyka bezpieczeństwa;

b) Pierwsza zasada – zarządzanie ryzykiem bezpieczeństwa;

c) Druga zasada – prawdopodobieństwo ryzyka bezpieczeństwa;

d) Trzecia zasada – dotkliwość ryzyka bezpieczeństwa;

e) Czwarta zasada – tolerancja ryzyka bezpieczeństwa;

f) Piąta zasada – kontrola/łagodzenie ryzyka bezpieczeństwa;

g) Pięć zasad zarządzania ryzykiem bezpieczeństwa – podsumowanie.

## 5.2 DEFINICJA RYZYKA BEZPIECZEŃSTWA

5.2.1 Rozdział 2 podręcznika definiuje bezpieczeństwo jako wynik zarządzania wieloma procesami organizacyjnymi. Zarządzanie tymi procesami ma na celu utrzymywanie ryzyka bezpieczeństwa pod organizacyjną kontrolą. Kluczowym w tym ujęciu jest postrzeganie bezpieczeństwa jako wyniku i zarządzania ryzykiem jako procesu.

5.2.2 Rozdział 4 podręcznika omawiał identyfikację zagrożeń jako jedną z dwóch głównych czynności wspierających zarządzanie bezpieczeństwem. Identyfikacja zagrożeń odnosi się także do solidności w prowadzeniu innych procesów, niebezpośrednio związanych z zarządzaniem ryzykiem. W kolejności, do zapewnienia właściwej identyfikacji i analizy zagrożeń, rozdział 4 ustanawia jasny podział pomiędzy zagrożeniami, jako źródłami potencjalnych obrażeń lub uszkodzeń oraz jego konsekwencjami dla bezpieczeństwa opisanymi pod względem operacyjnym.

5.2.3 Zarządzanie ryzykiem bezpieczeństwa jest główną działalnością, która wspiera zarządzanie bezpieczeństwem i odnosi się do innych niebezpośrednio związanych procesów organizacyjnych. Termin zarządzanie bezpieczeństwem w przeciwieństwie do bardziej ogólnego terminu zarządzanie ryzykiem, ma za zadanie podkreślić, że termin "zarządzanie bezpieczeństwem" nie dotyczy (bezpośrednio) zarządzania ryzykiem finansowym, prawnym, ekonomicznym, itd., ale ogranicza się przede wszystkim do zarządzania ryzykiem bezpieczeństwa.

5.2.4 Powszechnym problemem jest to, że czynności związane z zarządzaniem bezpieczeństwem często nie wykraczają poza identyfikację i analizę zagrożeń, lub, w innych przypadkach, przeskakują z identyfikacji zagrożeń bezpośrednio do wprowadzania elementów łagodzących ryzyko, omijając ocenę i określanie priorytetów ryzyka bezpieczeństwa jako konsekwencji zagrożeń. Mimo to, gdy raz zidentyfikowane źródła niebezpieczeństw lub szkód oraz ich konsekwencje zostały przeanalizowane i uzgodnione, strategie łagodzenia ryzyka zagrożeń, chroniące przed konsekwencjami, mogą być oczywiście wdrożone. To działanie będzie prawidłowe jeśli będzie stosowane z zasadą „bezpieczeństwo jako podstawowy priorytet” i będzie skupione na zapobieganiu negatywnych następstw. Jednakże, pod pojęciem zarządzanie bezpieczeństwem, uzgadnianie konsekwencji

zidentyfikowanych zagrożeń i opisywanie ich pod względem operacyjnym jest niewystarczające, by zapoczątkować proces łagodzenia zagrożeń. Koniecznym jest przeprowadzenie oceny wagi konsekwencji, by zdefiniować priorytety dla alokacji zasobów, podczas projektowania strategii zmniejszania zagrożeń.

5.2.5 Został zaproponowany podstawowy aforyzm zarządzania, mówiący że „nie można zarządzać czymś czego się nie zmierzy". Dlatego też, niezbędna jest uważna analiza,(pomiar) wagi konsekwencji zagrożeń. To jest zasadniczy wpływ zarządzania ryzykiem na zarządzanie bezpieczeństwem. Przez „numerowanie" (szeregowanie, porządkowanie) konsekwencji zagrożeń, proces zarządzania bezpieczeństwem prowadzi organizację z bazowymi zasadami dla decyzji związanych z ryzykiem bezpieczeństwa, a następnie alokacją zasobów organizacyjnych, służących zahamowaniu możliwości wystąpienia strat powodowanych zagrożeniami. Tym sposobem zarządzanie ryzykiem bezpieczeństwa uzupełnia podstawową „trylogię" zarządzania bezpieczeństwem: zagrożenia – konsekwencje – ryzyko bezpieczeństwa. To bezpośrednio wspiera rozwiązanie "dylematu dwóch P" omawianego w rozdziale 3.

5.2.6 Ryzyko, w wąskim jak i w szerokim rozumieniu, było przedmiotem wielu dyskusji i było opisywane w wielu publikacjach. Możliwa jest w tym przypadku pomyłka, wynikająca częściowo z powodu potocznego rozumienia terminu, który jest ciągle nadużywany, dość szeroki i generalnie rozmyty. Pierwszym krokiem do rozwiązania problemu tych pomyłek jest ograniczenie użycia ogólnego terminu ryzyko do bardziej konkretnego terminu „ryzyko bezpieczeństwa". Poza tym, jest to niezbędne by od samego początku ustanowić jasną definicję ryzyka bezpieczeństwa i połączyć tę definicję z pojęciem zagrożeń i konsekwencji wyrażonych w terminach operacyjnych.

5.2.7 Nawet po zawężeniu użycia podstawowego terminu ryzyko, do bardziej szczegółowego terminu ryzyko bezpieczeństwa, nieporozumienia mogą się ciągle pojawiać. Spowodowane to jest tym, że pojęcie ryzyka jest czymś sztucznym. Ryzyko bezpieczeństwa nie jest namacalnym czy możliwym do zobaczenia składnikiem fizycznego środowiska naturalnego. By zrozumieć lub wyobrazić sobie ryzyko bezpieczeństwa koniecznym jest użycie logicznego myślenia. Z drugiej strony, zagrożenia i ich konsekwencje są namacalnymi i widocznymi składnikami fizycznego środowiska naturalnego i dlatego też są intuicyjne w zakresie zrozumienia i wyobrażenia. Pojęcie ryzyko bezpieczeństwa jest tym, co jest znane jako konstrukcja, tj. sztuczna konwencja stworzona przez ludzi. Mówiąc prościej, kiedy zagrożenia i konsekwencje są fizycznymi komponentami świata naturalnego, ryzyko bezpieczeństwa tak naprawdę nie występuje w środowisku naturalnym. Ryzyko bezpieczeństwa jest wytworem ludzkiego rozumu, wymyślonym do mierzenia powagi, „szeregowania" konsekwencji zagrożeń.

5.2.8 Ryzyko bezpieczeństwa zostało zdefiniowane jako ocena wyrażona w przewidywanym prawdopodobieństwie i dotkliwości konsekwencji wystąpienia zagrożeń, biorąca jako punkt odniesienia najgorszą, dającą się przewidzieć sytuację. Normalnie ryzyka bezpieczeństwa są oznaczane w alfanumerycznej konwencji, która pozwala na ich mierzenie. Używając przykładu bocznego wiatru omawianego w rozdziale 4, można zauważyć, że proponowana definicja ryzyka bezpieczeństwa pozwala połączyć ryzyko bezpieczeństwa z zagrożeniami i konsekwencjami, a w ten sposób zamyka pętlę „trylogii" zagrożeń – konsekwencji – ryzyka bezpieczeństwa:

a) wiatr o prędkości 15 węzłów wiejący w poprzek drogi startowej jest zagrożeniem;

b) możliwość wypadnięcia w bok z drogi startowej spowodowanej tym, że pilot nie będzie w stanie utrzymać kierunku poruszania się statku powietrznego w czasie startu lub lądowania, jest jedną z konsekwencji zagrożenia;

c) ocena konsekwencji wypadnięcia z drogi startowej, wyrażona w prawdopodobieństwie i dotkliwości, za pomocą układu alfanumerycznego, jest ryzykiem bezpieczeństwa.

### 5.3 PIERWSZA ZASADA – ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA

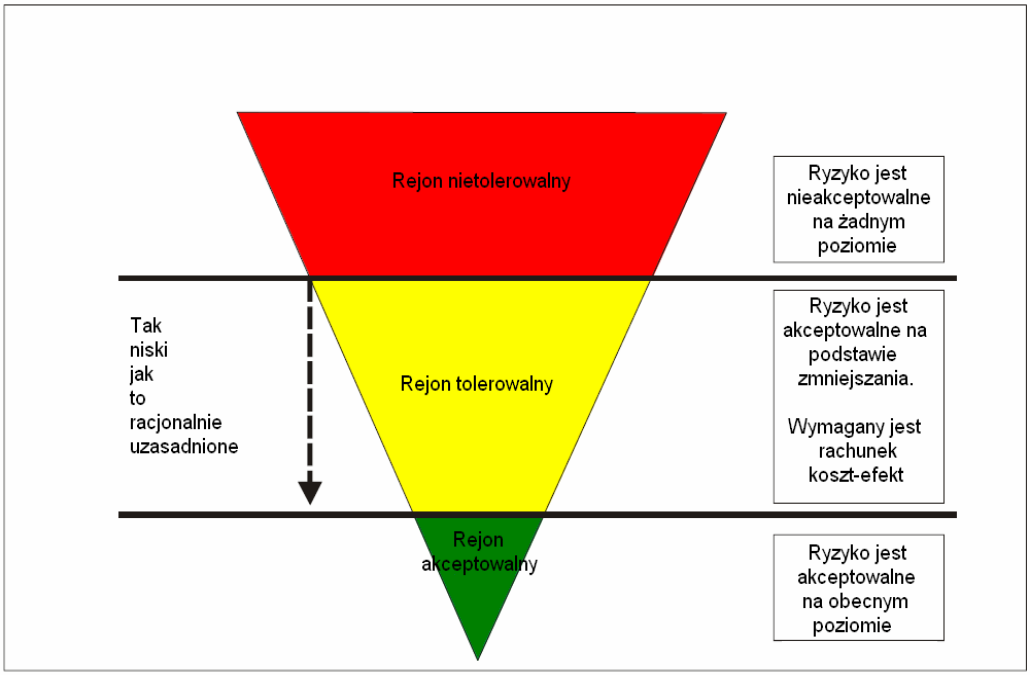
5.3.1 Zarządzanie ryzykiem bezpieczeństwa jest ogólnym terminem zawierającym ocenę i łagodzenie ryzyka bezpieczeństwa konsekwencji zagrożeń dla organizacji, do poziomu najniższego z możliwych (*as low as reasonably practicable - ALARP*). Celem zarządzania ryzykiem bezpieczeństwa jest zapewnić podstawy pod zbalansowaną alokację zasobów pomiędzy wszystkimi ocenionymi ryzykami dla bezpieczeństwa i tymi ryzykami bezpieczeństwa, których kontrola i łagodzenie jest wykonalne. Innymi słowy, jest to analiza zarządzania ryzykiem bezpieczeństwa w rozwiązywaniu "dylemat dwóch P". Zarządzanie ryzykiem bezpieczeństwa jest zatem kluczowym składnikiem procesu zarządzania bezpieczeństwem. Jego wartość dodana, jednakże polega na tym, że jest to podejście do alokacji zasobów oparte na danych, a więc możliwe do obronienia i łatwiejsze do wyjaśnienia.

5.3.2 Ilustracja 5-1 pokazuje ogólnie przyjętą prezentację graficzną procesu zarządzania ryzykiem. Odwrócony trójkąt wskazuje, że lotnictwo (tak jak inne socjotechniczne systemy produkcyjne) jest „ciężkie u góry", patrząc z perspektywy ryzyka bezpieczeństwa: większość ryzyk dla bezpieczeństwa, jako konsekwencji zagrożeń będzie wstępnie oceniane jako trafiające w rejon nietolerowany. Mniejsza liczba ryzyk dla bezpieczeństwa będzie oceniona w ten sposób, że znajdzie się w rejonie tolerowalnym, natomiast najmniejsza liczba będzie oceniona i znajdzie się bezpośrednio w rejonie akceptowalnym.

5.3.3 Ryzyka bezpieczeństwa ocenione jako początkowo trafiające w rejon nietolerowalny są nieakceptowalne pod żadnym warunkiem. Prawdopodobieństwo wystąpienia i/lub dotkliwość konsekwencji zagrożeń są bardzo duże. Szkodliwy potencjał ich zagrożeń stanowi takie zagrożenie dla przetrwania organizacji, że wzmagane są niezwłoczne czynności łagodzące ryzyko. Mówiąc ogólnie, dla organizacji dostępne są dwie możliwości, które mogą sprowadzić ryzyko bezpieczeństwa do tolerowalnego lub akceptowalnego rejonu:

a) alokacja zasobów by zredukować narażenie na, i/lub wielkość, szkodliwego potencjału konsekwencji zagrożeń; lub

b) jeśli złagodzenie ryzyka nie jest możliwe, zaprzestanie wykonywania operacji.




**Ilustracja 5-1. Zarządzanie ryzykiem bezpieczeństwa**

5.3.4 Ryzyka bezpieczeństwa oceniane jako początkowo trafiające w rejon tolerowalny są akceptowalne. Gwarantują to zapewniane strategie łagodzące ryzyko wprowadzone we właściwe miejsce. W przewidywalnym zakresie prawdopodobieństwo i/lub dotkliwość konsekwencji zagrożeń są utrzymywane pod kontrolą organizacyjną. Te same kryteria kontroli należy zastosować do ryzyk bezpieczeństwa wstępnie ocenionych jako nietolerowalne i złagodzone do poziomu tolerowalnego. Ryzyko bezpieczeństwa wstępnie ocenione jako nietolerowalne, które jest złagodzone i przesuwa się w dół do rejonu tolerowalnego musi pozostać „chronione" przez strategie łagodzące, które gwarantują ich kontrolę. W obu przypadkach wymagana jest analiza koszt-efekt:

a) Czy można osiągnąć zysk z inwestycji leżącej u podstaw alokacji zasobów, by objąć prawdopodobieństwo i/lub dotkliwość konsekwencji zagrożeń organizacyjną kontrolą? lub

b) Czy jest wymagana alokacja zasobów o takiej wielkości, która będzie stanowić większe zagrożenie dla rentowności organizacji niż objęcie prawdopodobieństwa i/lub dotkliwości konsekwencji zagrożeń kontrolą organizacyjną?

5.3.5 Akronim ALARP jest używany do opisania ryzyka bezpieczeństwa które zostało zredukowane do poziomu najniższego z możliwych . W określeniu „najniższy z możliwych", w kontekście zarządzania ryzykiem bezpieczeństwa, rozważane powinny być oba aspekty: technicznej wykonalności redukcji ryzyka bezpieczeństwa i kosztów. Działanie to musi zawierać analizę koszt-efekt. Osiągając to, że ryzykiem bezpieczeństwa w systemie jest ALARP oznacza, że żadne dalsze redukowanie ryzyka jest albo niewykonalne albo znacznie przeciążone kosztami. Jednakże powinno się pamiętać, że gdy organizacja „akceptuje" ryzyko bezpieczeństwa, to działanie nie oznacza, że ryzyko bezpieczeństwa zostało wyeliminowane. Niektóre szczątkowe poziomy ryzyka bezpieczeństwa pozostają. Skądinąd, organizacja przyjęła, że szczątkowe ryzyko bezpieczeństwa jest wystarczająco niskie tak, że jest przewyższane przez zyski.

5.3.6 Ryzyka bezpieczeństwa ocenione początkowo jako trafiające w rejon akceptowalny są akceptowalne na ich obecnym poziomie i nie wymagają działań zmierzających do umieszczenia lub zachowania ich prawdopodobieństwa i/lub dotkliwości konsekwencji pod organizacyjną kontrolę.

5.3.7 Analizy koszt-efekt leżą w sercu zarządzania ryzykiem bezpieczeństwa. Są dwa odrębne koszty, które są rozważane w analizie koszt-efekt: koszty bezpośrednie i koszty pośrednie.

5.3.8 ***Koszty bezpośrednie*** są kosztami oczywistymi i są dość proste do określenia. Odnoszą się głównie do fizycznych uszkodzeń i zawierają koszty naprawy, zastępstwa albo rekompensaty za obrażenia, uszkodzenia statku powietrznego/sprzętu lub mienia. Wysokie koszty leżące u podłoża utraty organizacyjnej kontroli nad pewnymi ekstremalnymi konsekwencjami zagrożeń (jak wypadek), mogą być redukowane przez ochronę ubezpieczeniową. Jednak należy pamiętać, że wykupienie ubezpieczenia nie powoduje wniesienia prawdopodobieństwa i/lub dotkliwości konsekwencji zagrożeń pod kontrolę organizacyjną. Ceduje jedynie ryzyko finansowe z organizacji na ubezpieczyciela. Ryzyka bezpieczeństwa pozostają nierozwiązane. Proste wykupienie ubezpieczenia do przekazania ryzyka finansowego trudno uznać za strategię zarządzania bezpieczeństwem.

5.3.9 ***Koszty pośrednie*** zawierają wszystkie koszty, które są pośrednio obejmowane ubezpieczeniem. Koszty te mogą wynosić więcej niż koszty bezpośrednie wynikające z utraty organizacyjnej kontroli z pewnych ekstremalnych konsekwencji zagrożeń. Takie koszty czasami są ukryte, ujawniają się często z opóźnieniem. Kilka przykładów nieubezpieczanych kosztów, które mogą prowadzić do utraty organizacyjnej kontroli nad ekstremalnymi konsekwencjami zagrożeń, to:

a) ***Utrata interesu i utrata reputacji organizacji.*** Wiele innych organizacji nie będzie pozwalało na korzystanie z usług linii lotniczej, która ma wątpliwe doświadczenia w zakresie bezpieczeństwa.

b) ***Utrata użycia sprzętu.*** Jest to utożsamiane z utratą dochodów. Sprzęt zastępczy może zostać zakupiony lub wyleasingowany. Przedsiębiorstwa operujące na jednym typie statku powietrznego mogą stwierdzić, że ich zapasowe, dodatkowe zasoby i personel wyspecjalizowany w obsłudze tego statku powietrznego będą w nadmiarze.

c) ***Utrata możliwości produkcyjnych personelu.*** Jeżeli pracownicy doznali obrażeń i w konsekwencji nie mogą pracować, prawo pracy może wymagać jakichś form rekompensat dla poszkodowanych. Również poszkodowany personel będzie musiał zostać zastąpiony, co najmniej na krótki czas, co wiąże się z dodatkowymi kosztami płac, szkoleń, nadgodzin, jak również ze znacznym wzrostem obciążenia pracą doświadczonego personelu.

d) ***Badanie i porządkowanie.*** Te koszty są często nieubezpieczone. Operatorzy mogą ponieść koszty badania zdarzenia zawierające koszty udziału personelu w badaniu jak również koszty badań i analiz, odzyskania szczątków, czy uprzątnięcia miejsca zdarzenia.

e) ***Odliczenia ubezpieczeniowe.*** Ubezpieczony może być zobligowany do pokrycia pierwszej części kosztów jakiegokolwiek zdarzenia. Roszczenie może także wnieść przedsiębiorstwo w wyższą kategorię ryzyka ubezpieczeniowego i dlatego może skutkować podwyższonymi opłatami (i odwrotnie, wprowadzenie działań redukujących z zakresu bezpieczeństwa, może pomóc wynegocjować niższe opłaty).

f) ***Wystąpienie na drogę sądową i roszczenia dotyczące uszkodzeń.*** Koszty prawne mogą narastać lawinowo. Podczas gdy możliwe jest ubezpieczenie od odpowiedzialności cywilnej i od uszkodzeń, praktycznie niemożliwe jest pokrycie kosztów czasu straconej operacji, powództw sądowych i roszczeń dotyczących uszkodzeń.

g) ***Grzywny i pozwy.*** Władze państwa mogą nakładać grzywny i pozywać oraz prawdopodobnie likwidować niebezpieczne operacje.

5.3.10 Wyniki analiz koszt-efekt mogą być numerycznie sprecyzowane i analitycznie dokładne. Niemniej, znajdują się tam mniej dokładne czynniki numeryczne, rozważane w analizie koszt-efekt. Te czynniki to:

a) ***Kierowniczy.*** Czy ryzyko bezpieczeństwa jest spójne z polityką bezpieczeństwa i celami organizacji?

b) ***Prawny.*** Czy ryzyko bezpieczeństwa jest zgodne z aktualnymi prawnymi standardami i możliwościami ich wprowadzenia?

c) ***Kulturowy.*** Jak personel organizacji i partnerzy będą patrzyli na ryzyko bezpieczeństwa?

d) ***Rynkowy.*** Czy walka rynkowa i dobro organizacji w porównaniu do innych podmiotów będzie narażać ryzyko bezpieczeństwa?

e) ***Polityczny.*** Czy będą polityczne koszty niepodejmowania tematu ryzyka bezpieczeństwa?

f) ***Publiczny.*** Jak wpływowe będą media lub grupy szczególnych interesów w kształtowaniu opinii publicznej dotyczącej ryzyka bezpieczeństwa?

## 5.4 DRUGA ZASADA — PRAWDOPODOBIEŃSTWO RYZYKA BEZPIECZEŃSTWA

5.4.1 Proces wprowadzania ryzyka bezpieczeństwa pod organizacyjną kontrolę zaczyna się oceną możliwości, czy konsekwencje zagrożeń zmaterializują się w czasie operacji, której celem jest dostarczanie usług. Jest to znane jako ocena prawdopodobieństwa ryzyka bezpieczeństwa.

5.4.2 Prawdopodobieństwo wystąpienia ryzyka bezpieczeństwa jest definiowane jako realność wystąpienia niebezpiecznego wydarzenia lub okoliczności. W definiowaniu realności prawdopodobieństwa mogą być pomocne pytania takie jak:

a) Czy w przeszłości wystąpiły podobne zdarzenia do tego rozważanego, czy jest to odosobniony przypadek?

b) Jaki inny sprzęt lub części tego samego typu mogą mieć podobne defekty?

c) Jak duża część personelu jest zaangażowana lub podlega rozważanej procedurze?

d) Przez jaki procent czasu potencjalnie niebezpieczny sprzęt lub procedura jest w użyciu?

e) Do jakiego stopnia rozrośnięte są implikacje wynikające z zarządzania, organizacyjne lub regulacyjne, które mogą mieć swoje odzwierciedlenie w większym zagrożeniu dla bezpieczeństwa publicznego?

5.4.3 Żaden lub wszystkie z czynników leżących u podstawy tych przykładowych pytań mogą być istotne, co podkreśla wagę rozważań wielowątkowych. W ocenianiu realności prawdopodobieństwa, że niebezpieczne wydarzenie lub okoliczność może się wydarzyć, wszystkie potencjalnie istotne perspektywy muszą być ocenione.

5.4.4 W ocenianiu realności prawdopodobieństwa, że niebezpieczne wydarzenie lub okoliczność może się wydarzyć, odniesienie do danych z przeszłości zawartych w „archiwum bezpieczeństwa" organizacji jest nadrzędne w procesie podjęcia przemyślanej decyzji. Idąc tą drogą, organizacja, która nie posiada „archiwum bezpieczeństwa" może przeprowadzić tylko ocenę prawdopodobieństwa opartą na trendach przemysłowych (w najlepszym przypadku) lub opartą na opiniach (w najgorszym).

5.4.5 Bazując na rozważaniach wynikających z odpowiedzi na pytania wymienione w punkcie 5.4.2, prawdopodobieństwo, że niebezpieczne zdarzenie lub okoliczność może się zdarzyć, może być ustanowione i jego znaczenie może być ocenione przy użyciu tabeli prawdopodobieństwa wystąpienia ryzyka.

5.4.6 Ilustracja 5-2 prezentuje typową tabelę prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa, w tym przypadku pięciopunktową. Tabela zawiera pięć kategorii oznaczających prawdopodobieństwo wystąpienia niebezpiecznego zdarzenia lub okoliczności oraz znaczenie każdej kategorii i przydział wartości dla każdej kategorii. Należy podkreślić, że jest to przykład przedstawiony tylko dla celów edukacyjnych. Chociaż ta tabela, jak również tabela dotkliwości oraz macierze oceny ryzyka i tolerowalności, omawiane w następnych podpunktach są, mówiąc pojęciowo, standardami przemysłowymi; poziom uszczegółowienia i kompleksowość tabel i macierzy muszą być zaadaptowane i współmierne do konkretnych potrzeb i złożoności różnych organizacji. Są organizacje, które zawierają oba sposoby określania: jakościowe i ilościowe. Podobnie, niektóre tabele rozrastają się do piętnastu punktów. Pięciopunktowe tabele i macierze „pięć na pięć" nie powinny być rozumiane jako standardowe. Zostały one jedynie uznane jako kompleksowe i jako takie są odpowiednie do celów edukacyjnych jak również dla potrzeb tego podręcznika.

### 5.5 TRZECIA ZASADA — DOTKLIWOŚĆ RYZYKA BEZPIECZEŃSTWA

5.5.1 Po pierwsze ryzyko niebezpiecznego wydarzenia lub okoliczności zostało ocenione w terminach możliwości wystąpienia. Drugi krok, w procesie roztaczania organizacyjnej kontroli nad ryzykiem bezpieczeństwa, to ocena dotkliwości konsekwencji zagrożenia, jeśli jego potencjał niszczący się zmaterializuje podczas operacji nastawionych na dostarczanie usług. Jest to znane jako ocenianie dotkliwości ryzyka bezpieczeństwa.

| | Znaczenie | Wartość |
|---|---|---|
| **Częste** | Prawdopodobnie wystąpi często (występowało często) | **5** |
| **Sporadyczne** | Prawdopodobnie wystąpi sporadycznie (występowało sporadycznie) | **4** |
| **Niewielkie** | Prawdopodobnie nie wystąpi, ale jest to możliwe (występowało rzadko) | **3** |
| **Nieprawdopodobne** | Bardzo mało prawdopodobne, że wystąpi (nie znany jest przypadek by wystąpiło) | **2** |
| **Skrajnie nieprawdopodobnie** | Prawie niewyobrażalne, że kiedykolwiek może wystąpić | **1** |

**Ilustracja 5-2. Tabela prawdopodobieństwa ryzyka bezpieczeństwa**

5.5.2 Dotkliwość ryzyka bezpieczeństwa jest definiowana jako możliwe konsekwencje wystąpienia niebezpiecznego wydarzenia lub okoliczności, biorąc jako punkt odniesienia najgorszą możliwą do przewidzenia sytuację. Ocenę dotkliwości konsekwencji zagrożenia, jeśli jego potencjał niszczący się zmaterializuje podczas operacji nastawionych na dostarczanie usług można wspomóc pytaniami:

a) Jak wiele może być ofiar (pracowników, pasażerów, świadków i osób postronnych)?

b) Jaki jest przypuszczalny rozmiar strat materialnych lub finansowych (bezpośrednie straty sprzętowe operatora, uszkodzenia infrastruktury lotniczej, straty stron trzecich, wpływ na finanse i gospodarkę krajową)?

c) Jakie jest prawdopodobieństwo negatywnego wpływu na środowisko (rozlanie paliwa lub innych substancji niebezpiecznych, fizyczne zniszczenia siedlisk naturalnych)?

d) Jakie są prawdopodobne konsekwencje polityczne i/lub zainteresowanie mediów?

5.5.3 Bazując na rozważaniach wynikających z odpowiedzi na pytania, takie jak te wymienione w punkcie 5.5.2, dotkliwość możliwych konsekwencji niebezpiecznego wydarzenia lub okoliczności, biorąc jako punkt odniesienia najgorszą możliwą do przewidzenia sytuację, może być oceniana przy użyciu tabeli dotkliwości ryzyka bezpieczeństwa.

5.5.4 Ilustracja 5-3 prezentuje typową tabelę dotkliwości ryzyka bezpieczeństwa, także pięciopunktową. Tabela zawiera pięć kategorii opisujących poziom dotkliwości niebezpiecznego zdarzenia lub okoliczności, znaczenie każdej kategorii i przydział wartości dla każdej kategorii. Tak samo jak tabela prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa, ta tabela jest przykładem prezentowanym tylko dla celów edukacyjnych i zastrzeżenie zawarte w punkcie 5.4.6 ma w tym przypadku również zastosowanie.

| Dotkliwość zdarzenia | Znaczenie | Wartość |
|---|---|---|
| Katastrofalna | — Wiele ofiar<br>— Zniszczenie sprzętu | A |
| Niebezpieczna | — Duże obniżenie marginesu bezpieczeństwa, niemożność polegania na operatorach, by wykonywali obowiązki dokładnie i kompletnie ze względu na fizyczne obrażenia lub natłok pracy<br>— Poważne obrażenia ciała<br>— Duże straty w sprzęcie | B |
| Poważna | — Znaczne obniżenie marginesu bezpieczeństwa, natłok pracy lub warunki osłabiające wydajność operatorów, skutkujące ograniczeniem ich zdolności do radzenia sobie w niekorzystnych sytuacjach/warunkach<br>— Poważny incydent<br>— Obrażenia ciała | C |
| Niewielka | — Uciążliwość<br>— Ograniczenia operacyjne<br>— Użycie procedur awaryjnych<br>— Incydenty | D |
| Nieistotna | — Małe konsekwencje | E |

**Ilustracja 5-3. Tabela dotkliwości ryzyka bezpieczeństwa**

### 5.6 CZWARTA ZASADA — TOLERANCJA RYZYKA BEZPIECZEŃSTWA

5.6.1 Kiedy już ryzyko bezpieczeństwa konsekwencji niebezpiecznego wydarzenia lub okoliczności zostało ocenione w kategoriach możliwości i dotkliwości jego wystąpienia, trzecim krokiem, w procesie sprawowania organizacyjnej kontroli nad ryzykiem bezpieczeństwa i wystąpienia konsekwencji niebezpiecznego wydarzenia lub okoliczności, jest ocena tolerancji względem konsekwencji zagrożenia, jeżeli jego potencjał niszczący ujawni się podczas operacji nastawionej na dostarczanie usług. Jest to znane jako ocena tolerancji ryzyka bezpieczeństwa i jest to proces dwustopniowy.

5.6.2 Pierwszy stopień. Niezbędne jest otrzymanie całkowitej oceny ryzyka bezpieczeństwa. Jest to osiągane przez złożenie tabeli prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa i tabeli dotkliwości ryzyka bezpieczeństwa w macierz oceny ryzyka bezpieczeństwa. Taka przykładowa macierz jest zaprezentowana na ilustracji 5-4. Na przykład prawdopodobieństwo wystąpienia ryzyka bezpieczeństwa zostało ocenione jako sporadyczne (4), a dotkliwość ryzyka bezpieczeństwa jako niebezpieczne (B). Połączenie możliwości wystąpienia i dotkliwości (4B) jest ryzykiem bezpieczeństwa konsekwencji zagrożenia branego pod rozwagę. Rozwijając dyskusję z podrozdziału 5.2, przez ten przykład można zobaczyć, że ryzyko to jest tylko numerem lub kombinacją alfanumeryczną i nie jest widzialną lub namacalną częścią świata naturalnego. Kolory w macierzy z ilustracji 5-4 odzwierciedlają rejony z odwróconego trójkąta z ilustracji 5-1.

5.6.3 Drugi stopień, wskaźnik ryzyka bezpieczeństwa uzyskany z macierzy oceny ryzyka bezpieczeństwa musi być eksportowany do macierzy tolerowalności ryzyka bezpieczeństwa, która opisuje kryteria tolerancji. Kryterium dla ryzyka bezpieczeństwa ocenionego jako 4B jest, zgodnie z tabelą tolerancji z ilustracji 5-5, „nieakceptowalne przy istniejących okolicznościach". W tym wypadku ryzyko bezpieczeństwa trafia w nietolerowalny rejon odwróconego trójkąta. Ryzyko bezpieczeństwa wystąpienia konsekwencji zagrożeń jest nieakceptowalne. Organizacja musi:

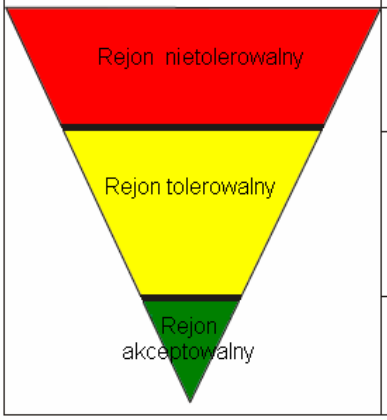
a) alokować zasoby, by zredukować nastawienie na konsekwencje zagrożeń;

b) alokować zasoby, by zredukować wielkość potencjału niszczącego konsekwencji zagrożeń; lub

c) zaprzestać wykonywania operacji, jeśli złagodzenie ryzyka nie jest możliwe.

| Prawdopodobieństwo ryzyka | | Dotkliwość ryzyka | | | | |
|---|---|---|---|---|---|---|
| | | Katastrofalna A | Niebezpieczna B | Poważna C | Niewielka D | Nieistotna E |
| Częste | 5 | 5A | 5B | 5C | 5D | 5E |
| Sporadyczne | 4 | 4A | 4B | 4C | 4D | 4E |
| Niewielkie | 3 | 3A | 3B | 3C | 3D | 3E |
| Nieprawdopodobne | 2 | 2A | 2B | 2C | 2D | 2E |
| Skrajnie nieprawdopodobne | 1 | 1A | 1B | 1C | 1D | 1E |

**Ilustracja 5-4. Macierz oceny ryzyka bezpieczeństwa**

| Sugerowane kryteria | Indeks oceny ryzyka | Sugerowane kryteria |
|---|---|---|
|  | **5A, 5B, 5C, 4A, 4B, 3A** | Nieakceptowalne przy obecnych okolicznościach |
| | **5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C** | Akceptowalne na podstawie środków łagodzących ryzyko.<br><br>Może to wymagać decyzji kierowniczych. |
| | **3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E** | Akceptowalne |

**Ilustracja 5-5. Macierz tolerancji ryzyka bezpieczeństwa**

## 5.7 PIĄTA ZASADA — KONTROLA/ŁAGODZENIE RYZYKA BEZPIECZEŃSTWA

5.7.1 W piątym i ostatnim kroku procesu wprowadzania ryzyka bezpieczeństwa pod kontrolę organizacyjną, muszą być wprowadzone strategie kontroli/łagodzenia ryzyka. Mówiąc ogólnie, kontrola i łagodzenie są terminami, które mogą być używane wymiennie. Oba zmierzają do wyznaczenia mierników odnoszących się do zagrożeń oraz do wprowadzenia prawdopodobieństwa wystąpienia ryzyka bezpieczeństwa i dotkliwości konsekwencji zagrożeń pod organizacyjną kontrolę.

5.7.2 Kontynuując z przykładem z punktu 5.6, rozważane ryzyko bezpieczeństwa konsekwencji zagrożeń zostało ocenione jako 4B („nieakceptowalne przy istniejących okolicznościach”). Zasoby muszą więc być alokowane by „zsunąć” je w dół trójkąta, w rejon tolerowalny, gdzie ryzyka bezpieczeństwa są ALARP. Jeśli to nie może być osiągnięte, to operacja nastawiona na dostarczanie usług, która naraża organizację na konsekwencje zagrożeń musi być zaniechana. Ilustracja 5-6 prezentuje proces zarządzania w formie graficznej.

5.7.3 Istnieją trzy podstawowe strategie kontroli/łagodzenia ryzyka bezpieczeństwa:

a) ***Unikanie.*** Operacja lub działalność jest zarzucana z powodu tego, że ryzyko przewyższa zyski z kontynuowania operacji lub działalności. Przykładowe strategie unikania to:

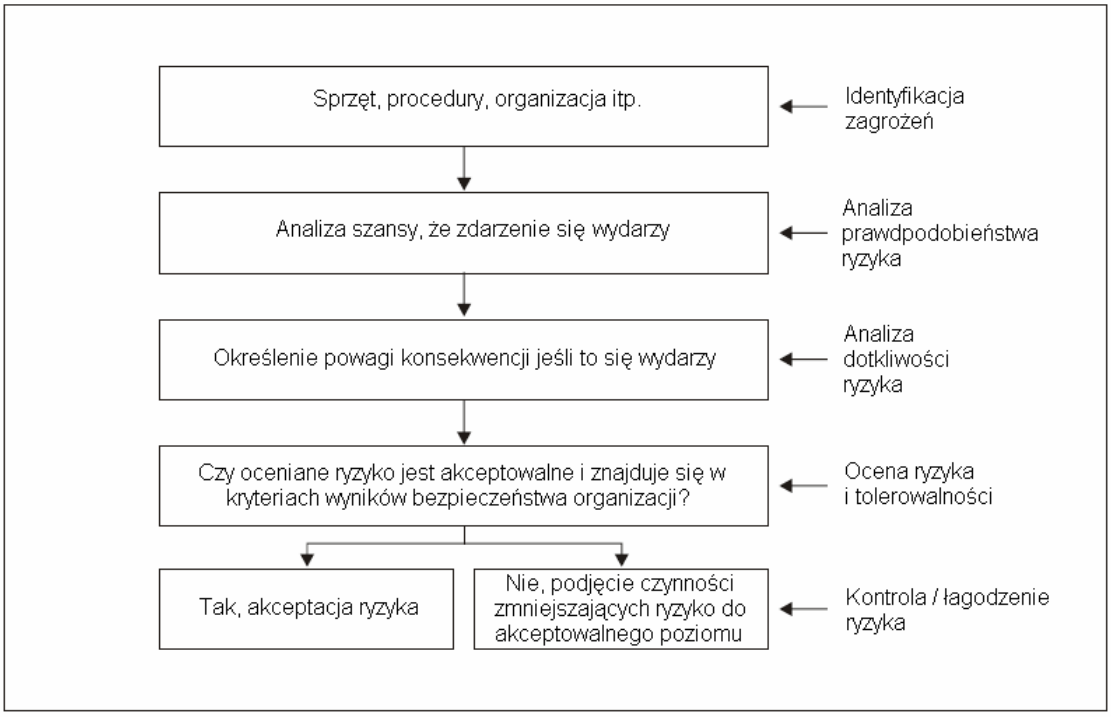
1) operacje na lotnisku ze skomplikowanym otoczeniem geograficznym, bez niezbędnych pomocy nawigacyjnych, są zarzucane.

2) operacje w przestrzeni RVSM, statkiem powietrznym niewyposażonym do lotów RVSM, są zarzucane.

b) ***Redukcja.*** Częstotliwość operacji lub działalności jest redukowana lub podejmowane są czynności zmierzające do redukcji wagi konsekwencji zaakceptowanych ryzyk. Przykładowe strategie redukcji to:

1) operacje na lotnisku ze skomplikowanym otoczeniem geograficznym, bez niezbędnych pomocy nawigacyjnych, są ograniczone do lotów dziennych, w warunkach VMC.

2) operacje statkiem powietrznym niewyposażonym do lotów RVSM są przeprowadzane powyżej lub poniżej przestrzeni RVSM.




**Ilustracja 5-6. Proces zarządzania ryzykiem bezpieczeństwa**

c) ***Segregacja narażenia.*** Podejmowane są czynności zmierzające do odizolowania skutków konsekwencji zagrożeń lub włączenia czynników redukcji, do ochrony przed nimi. Przykłady strategii opartych na segregacji narażenia to:

1) operacje na lotnisku ze skomplikowanym otoczeniem geograficznym, bez niezbędnych pomocy nawigacyjnych, są ograniczane do operacji przeprowadzanych przez statki powietrzne z określonymi możliwościami wyposażenia nawigacyjnego.

2) statek powietrzny niewyposażony do lotów RVSM nie jest dopuszczany do lotów w przestrzeni RVSM.

5.7.4 W ewaluowaniu konkretnych alternatyw służących łagodzeniu ryzyka bezpieczeństwa, należy pamiętać, że nie wszystkie mają ten sam potencjał redukujący ryzyko bezpieczeństwa. Efektywność każdej konkretnej alternatywnej metody wymaga ewaluacji przed podjęciem decyzji. Jest istotnym, by pełny zakres możliwych wskaźników kontrolnych i kompromis pomiędzy miernikami były rozważane w celu znalezienia optymalnego rozwiązania. Każda proponowana opcja łagodząca powinna być sprawdzona z takich perspektyw jak:

a) ***Efektywność.*** Czy będzie to redukowało czy eliminowało ryzyko bezpieczeństwa konsekwencji niebezpiecznego wydarzenia lub stanu? Do jakiego rozmiaru alternatywy będą łagodziły takie ryzyka? Efektywność może być widziana jako bycie w pewnym miejscu w kontinuum, jak poniżej:

1) ***Łagodzenie inżynieryjne.*** Ten sposób łagodzenia eliminuje ryzyko konsekwencji niebezpiecznego wydarzenia lub stanu, na przykład przez zastosowanie blokady by zapobiec włączeniu się odwracacza ciągu (rewersu) w locie.

2) ***Łagodzenie przez kontrolę.*** To łagodzenie akceptuje ryzyko w bezpieczeństwie konsekwencji niebezpiecznego wydarzenia lub stanu, ale reguluje system do łagodzenia takiego ryzyka przez redukowanie go do zarządzanego poziomu, na przykład przez nakładanie jeszcze bardziej restrykcyjnych warunków funkcjonowania. Oba aspekty, łagodzenie inżynieryjne i przez kontrolę, są uważane za „twarde" sposoby łagodzenia ryzyka, ponieważ nie są uzależnione od bezbłędnego wykonania przez człowieka.

3) ***Łagodzenie przez personel.*** To łagodzenie przyjmuje, że łagodzenie inżynieryjne i/lub przez kontrolę nie są ani wystarczające ani efektywne, więc personel musi być nauczony jak poradzić sobie z ryzykiem w bezpieczeństwie konsekwencji zagrożeń, na przykład przez dodanie ostrzeżeń, skorygowanych list kontrolnych, procedur operacyjnych i/lub dodatkowego treningu. Łagodzenie przez personel jest uznawane za „miękkie czynności", ponieważ jest uzależnione od bezbłędnego wykonania przez człowieka.

b) ***Koszt/efekt.*** Czy dostrzegalne zyski przewyższają koszty? Czy potencjał będzie przyrastał proporcjonalnie do wpływu zmian jakie są wymagane?

c) ***Praktyczność.*** Czy łagodzenie jest możliwe do zastosowania w praktyce i właściwe w warunkach dostępnych technologii, możliwości finansowych, możliwości administracyjnych, rządowych regulacji i prawa, woli politycznej, itd.?

d) ***Wyzwanie.*** Czy łagodzenie zniesie krytyczne spojrzenie każdego z zainteresowanych (pracowników, dyrektorów, akcjonariuszy, administracji państwowej, itd.)?

e) ***Akceptowalność dla każdego wspólnika.*** Jak dużego poziomu akceptacji (lub oporu) możemy się spodziewać ze strony wspólników? (Dyskusja ze wspólnikami podczas oceny ryzyka bezpieczeństwa może wskazać ich preferowany sposób łagodzenia ryzyka.)

f) ***Egzekwowalność.*** Jeśli są wprowadzane nowe zasady (procedury operacyjne, regulacje, itd.), czy są one do wyegzekwowania?

g) ***Trwałość.*** Czy łagodzenie ryzyka przetrwa próbę czasu? Czy będzie to czasowy zysk, czy przyniesie on użytek długoterminowy?

h) ***Pozostałość ryzyka bezpieczeństwa.*** Po zaimplementowaniu działań łagodzących, jakie ryzyko pozostanie z pierwotnego zagrożenia? Jaka jest możliwość by złagodzić to pozostałe, szczątkowe ryzyko?

i) ***Nowe problemy.*** Jakie nowe problemy lub nowe (możliwe, że gorsze) ryzyka bezpieczeństwa będą wprowadzone przez zaproponowane łagodzenie ryzyka?

5.7.5 Najbardziej efektywne łagodzenie ryzyka zamyka się w opisanych „twardych" metodach. Ponieważ „twarde" łagodzenie ryzyka jest często kosztowne, organizacje uciekają się do „miękkiego" łagodzenia (takiego jak trening). W takich przypadkach organizacja jest w większym stopniu odpowiedzialna za zarządzanie ryzykiem bezpieczeństwa, niż w przypadkach, w których odpowiedzialność nie jest przerzucana na pracowników.

5.7.6 Podsumowując, strategie kontroli/łagodzenia ryzyka bezpieczeństwa najczęściej bazują na wprowadzaniu kolejnych barier ochronnych,lub umacnianiu już istniejących. Bariery ochronne były omawiane w rozdziale 2 i przypomnijmy, że bariery ochronne w lotnictwie można pogrupować w trzy ogólne kategorie:

a) technologia;

b) trening;

c) regulacje.

5.7.7 Jako część kontroli/łagodzenia ryzyka bezpieczeństwa, ważny punkt stanowi określenie dlaczego nowe bariery ochronne są konieczne lub dlaczego istniejące muszą być wzmocnione. Poniższe pytania mogą dotyczyć takiego określania:

a) Czy bariery ochronne, chroniące przed ryzykiem bezpieczeństwa konsekwencji zagrożeń, istnieją?

b) Czy bariery ochronne funkcjonują jak planowano?

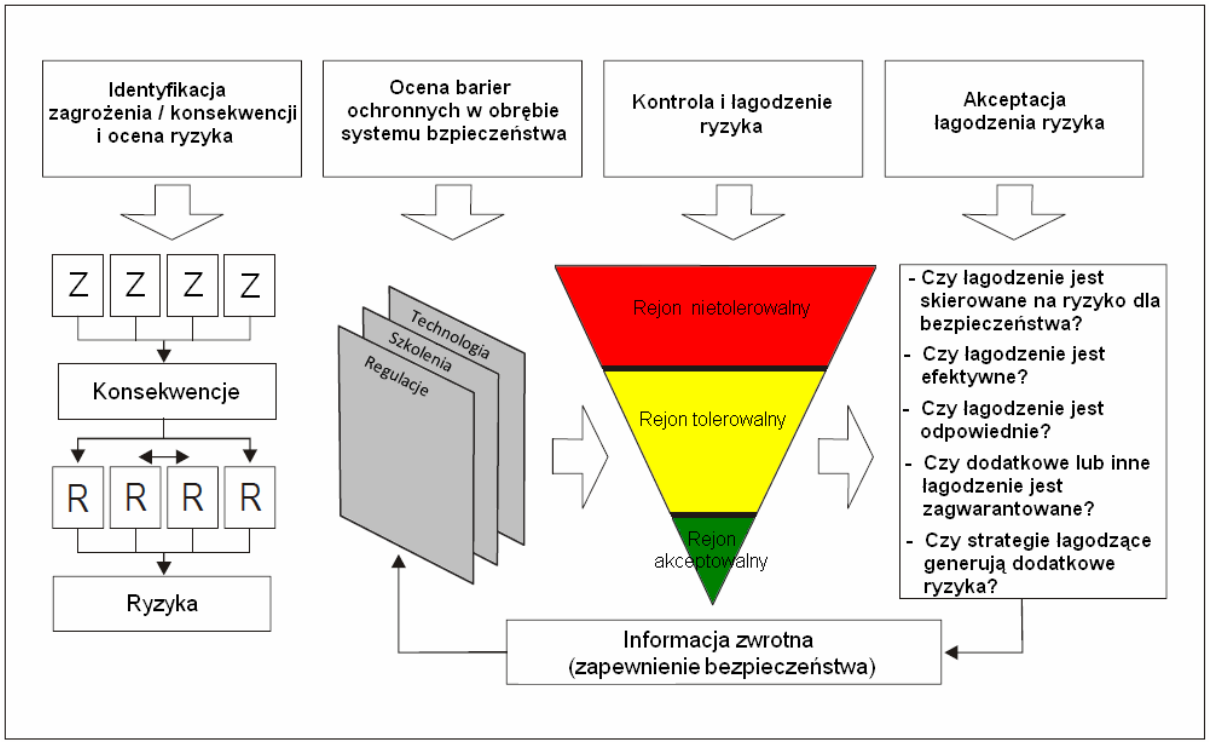
c) Czy bariery ochronne są praktyczne w użyciu przy aktualnych warunkach pracy?

d) Czy zaangażowany personel jest świadomy ryzyka bezpieczeństwa konsekwencji zagrożeń i bariery ochronne zostały wprowadzone?

e) Czy są wymagane dodatkowe mierniki dla łagodzenia/kontroli ryzyka bezpieczeństwa?

5.7.8 Ilustracja 5-7 prezentuje pełny proces łagodzenia ryzyka bezpieczeństwa w formie graficznej. Zagrożenia są potencjalną wrażliwością, w rozumieniu bezpieczeństwa, tkwiącymi w systemie lotniczym. Ta wrażliwość objawia się jako szeroki wachlarz konsekwencji. Żeby zarządzać bezpieczeństwem, niezbędnym jest przeprowadzenie oceny ryzyka bezpieczeństwa konsekwencji zagrożeń, poprzez przypisanie indeksu każdemu ryzyku. Każde zagrożenie może wygenerować jedną lub wiele konsekwencji i każda z nich może być oceniona w kontekście jednego lub wielu ryzyk dla bezpieczeństwa. Pierwszym krokiem w procesie łagodzenia/kontroli ryzyka bezpieczeństwa jest zatem identyfikacja zagrożeń/konsekwencji i ocena ryzyka bezpieczeństwa.

5.7.9 Kiedy zagrożenia i konsekwencje zostały zidentyfikowane, a ryzyko bezpieczeństwa ocenione, musi być oszacowana efektywność i sprawność istniejących w systemie lotniczym barier ochronnych (technologia, trening i regulacje) odnoszących się do zagrożeń i konsekwencji. Skutkiem tego działania będzie wzmocnienie istniejących barier ochronnych, budowa nowych barier lub obie te czynności. Drugim krokiem w procesie łagodzenia/kontroli ryzyka bezpieczeństwa jest zatem oszacowanie/ocena efektywności istniejących barier ochronnych wewnątrz systemu lotniczego.




**Ilustracja 5-7. Proces łagodzenia ryzyka bezpieczeństwa**

5.7.10 Bazując na wzmocnieniu istniejących barier ochronnych i/lub wprowadzaniu nowych, początkowe ryzyka bezpieczeństwa są ponownie oceniane by sprawdzić, czy są teraz tak niskie jak to racjonalnie uzasadnione. Trzecim krokiem w procesie łagodzenia/kontroli ryzyka bezpieczeństwa jest zatem działanie kontrolne/łagodzące ryzyko.

5.7.11 Przeprowadzając ponowną ocenę ryzyka bezpieczeństwa, efektywność i sprawność strategii kontroli/łagodzenia ryzyka musi być potwierdzona. Czwartym krokiem w procesie łagodzenia/kontroli ryzyka bezpieczeństwa jest akceptacja łagodzenia ryzyka bezpieczeństwa. Odnoszą się do tego poniższe pytania:

a) Czy łagodzenie jest skierowane na ryzyko bezpieczeństwa?

b) Czy łagodzenie jest efektywne?

c) Czy łagodzenie jest odpowiednie?

d) Czy dodatkowe lub inne łagodzenie jest zagwarantowane?

e) Czy strategie łagodzące generują dodatkowe ryzyka?

5.7.12 Kiedy łagodzenie ryzyka zostało zaakceptowane i rozwinięte, a strategie wdrożone jako część procesu zapewniania bezpieczeństwa, muszą być one zwrotnie wprowadzone w bariery ochronne organizacji na których strategie bazują, by zapewnić integralność, efektywność i sprawność tych barier w nowych warunkach operacyjnych.

## 5.8 PIĘĆ ZASAD ZARZĄDZANIA RYZYKIEM BEZPIECZEŃSTWA – PODSUMOWANIE

5.8.1 Ważne pojęcia odnoszące się do zarządzania ryzykiem bezpieczeństwa omawiane w tym rozdziale mogą być podsumowane następująco:

a) Nie ma takiej rzeczy jak bezpieczeństwo absolutne – w lotnictwie nie ma możliwości wyeliminowania wszystkich ryzyk bezpieczeństwa.

b) Ryzyko bezpieczeństwa musi być zmniejszone do poziomu najniższego z możliwych (ALARP).

c) Łagodzenie ryzyka bezpieczeństwa musi być zbalansowane w:

1) czasie;

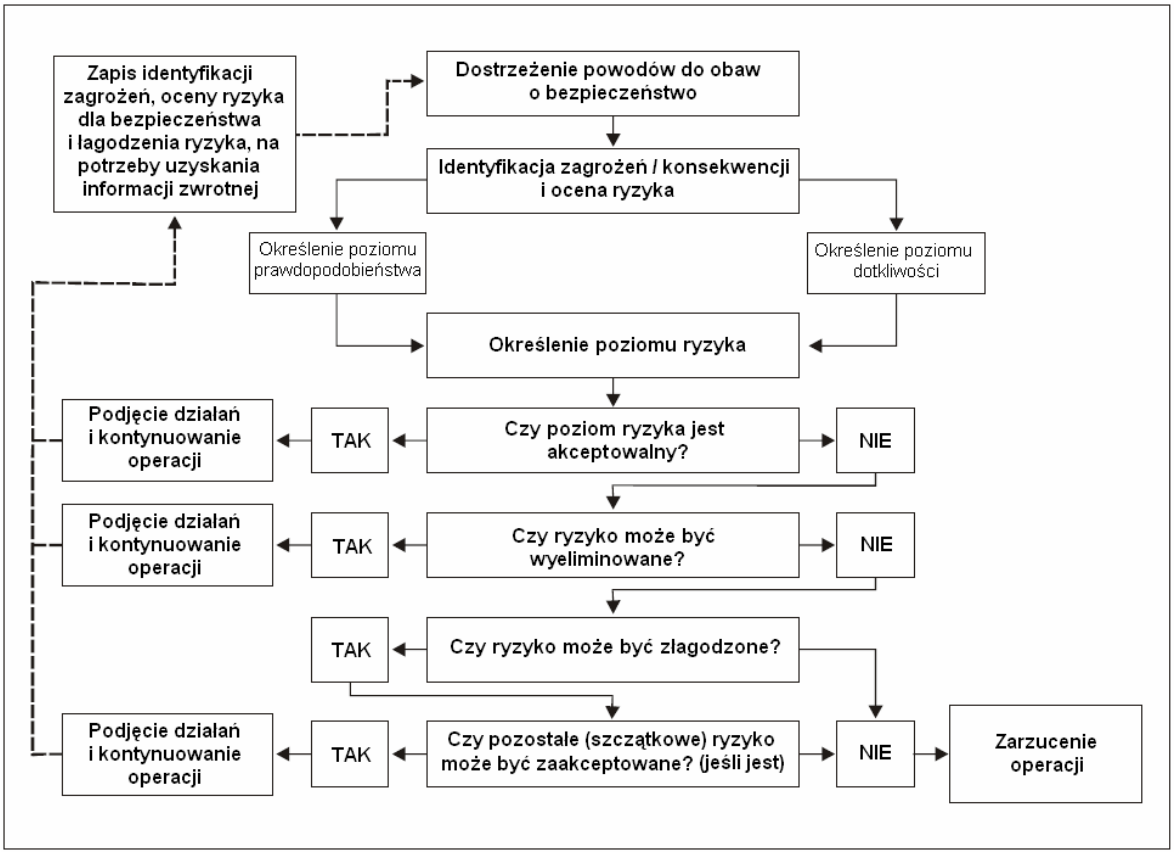
2) kosztach; oraz

3) trudnościach w pozyskiwaniu mierników służących do redukcji lub eliminacji ryzyka bezpieczeństwa (tj. zarządzania).

d) Efektywne zarządzanie ryzykiem bezpieczeństwa poszukuje maksymalizacji zysków z akceptacji ryzyka bezpieczeństwa (najczęściej redukcja albo czasu i/lub kosztów dostarczania usług) podczas minimalizacji samego ryzyka bezpieczeństwa.

e) Uzasadnienie dla decyzji związanych z ryzykiem bezpieczeństwa musi być przekazane wspólnikom, których one dotyczą, by zyskać ich akceptację.

5.8.2 Ilustracja 5-8 prezentuje proces zarządzania ryzykiem bezpieczeństwa w całości. Po dostrzeżeniu powodów do obaw o bezpieczeństwo, zagrożenia leżące u podstawy tych obaw i potencjalne konsekwencje zagrożeń są identyfikowane. Ryzyka bezpieczeństwa konsekwencji są ocenione pod względem możliwości wystąpienia i dotkliwości, w celu zdefiniowania poziomu ryzyka bezpieczeństwa (indeks ryzyka bezpieczeństwa). Jeśli ryzyka bezpieczeństwa są ocenione jako akceptowalne, właściwa czynność jest podejmowana i operacja jest kontynuowana. Dla celów związanych z zapewnieniem informacji zwrotnej rejestruje się identyfikację zagrożeń, ocenę ryzyka bezpieczeństwa i łagodzenie ryzyka.




**Ilustracja 5-8. Proces zarządzania ryzykiem bezpieczeństwa**

5.8.3 Jeśli ryzyka bezpieczeństwa są ocenione jako nieakceptowalne, poniższe pytania stają się istotne:

a) ***Czy ryzyko bezpieczeństwa może być wyeliminowane?*** Jeśli odpowiedź brzmi: tak, właściwa czynność jest podejmowana i informacja zwrotna trafia do „archiwum bezpieczeństwa". Jeśli odpowiedź brzmi: nie, to następne pytanie brzmi:

b) ***Czy ryzyko bezpieczeństwa może być złagodzone?*** Jeśli odpowiedź brzmi: nie, operacja musi zostać zarzucona. Jeśli odpowiedź brzmi: tak, właściwe czynności łagodzące ryzyko są podejmowane, a następnym pytaniem jest:

c) ***Czy pozostałe/szczątkowe ryzyko bezpieczeństwa może być zaakceptowane?*** Jeśli odpowiedź brzmi: tak, czynności są podejmowane (jeśli są konieczne) i informacja zwrotna trafia do „archiwum bezpieczeństwa". Jeśli odpowiedź brzmi: nie, operacja musi zostać odrzucona.

5.8.4 Pytanie 5.8.3 c) odzwierciedla fakt, że strategie łagodzące mogą nigdy całkowicie nie złagodzić ryzyka. Należy zaakceptować, że szczątkowe ryzyko bezpieczeństwa będzie istniało zawsze i organizacja musi upewnić się, że szczątkowe ryzyko jest także pod kontrolą.

5.8.5 W celu praktycznego zilustrowania procesu zarządzania ryzykiem bezpieczeństwa, trzy różne scenariusze zarządzania ryzykiem bezpieczeństwa są zaprezentowane w dodatkach do rozdziału. Dodatek 1 zawiera przykład ćwiczenia z zarządzania ryzykiem bezpieczeństwa na lotnisku. Dodatek 2 zawiera przykład ćwiczenia zarządzania ryzykiem bezpieczeństwa u dostawcy służb ruchu lotniczego. Dodatek 3 zawiera przykład ćwiczenia zarządzania ryzykiem bezpieczeństwa w linii lotniczej.

— — — — — — — — — —

## Dodatek 1 do Rozdziału 5

# PLAN ROZBUDOWY MIĘDZYNARODOWEGO PORTU LOTNICZEGO W ANYCITY

### 1. SCENARIUSZ

1.1 Międzynarodowy Port Lotniczy w Anycity (AIA) posiada dwie równoległe drogi startowe (główną i pomocniczą). Planowana jest budowa odwodnienia w pobliżu końca podejścia pomocniczej drogi startowej. Pojazdy budowlane muszą przeciąć główną drogę startową by dostać się na miejsce budowy. Z powodu dużego ruchu w ciągu dnia, podjęto decyzję, że prace będą wykonywane w nocy, kiedy ruch lotniczy jest mniejszy, by uniknąć zakłóceń w operacjach dziennych. Dyrektor ds. Bezpieczeństwa musi oszacować konsekwencje dla bezpieczeństwa wynikające z planu prowadzenia nocnych prac budowlanych.

1.2 Grupa Reagowania ds. Bezpieczeństwa (*Safety Action Group - SAG*) portu AIA otrzymała polecenie wsparcia Dyrektora ds. Bezpieczeństwa w oszacowaniu konsekwencji dla bezpieczeństwa wynikających z planu budowy. Jeden oczywisty i najpilniejszy obszar rozważań to ruch pojazdów do i z placu budowy, który może prowadzić do wtargnięć na drogę startową. SAG użyła procesu zarządzania ryzykiem bezpieczeństwa do oszacowania konsekwencji dla bezpieczeństwa wynikającego z planu budowy.

### 2. OPIS SYSTEMU

Jedno z pierwszych zadań Grupy Reagowania ds. Bezpieczeństwa (SAG) jest opisanie zmodyfikowanego systemu, w którym port lotniczy będzie przeprowadzał operacje, kiedy będą prowadzone prace budowlane, a więc:

a) otoczenie drogi startowej w czasie budowy w nocy, w tym duży ruch pojazdów budowy pomiędzy płytą lotniska a miejscem budowy;

b) istniejący program szkolenia kierowców i użycie eskorty dla pojazdów budowy;

c) wieża kontrolna i fakt braku łączności z pojazdami budowy (niewyposażonymi w radiostacje);

d) sygnały, oznaczenia i oświetlenie dróg kołowania, dróg startowych i terenu budowy.

### 3. PROCES IDENTYFIKACJI ZAGROŻEŃ

Drugim zadaniem SAG jest identyfikacja zagrożeń i ich możliwych konsekwencji, które mogą dotknąć operacji lotniskowych w czasie budowy, a więc:

a) Określić ogólne zagrożenia:

1) Projekt lotniska.

b) Określić szczegółowe komponenty zagrożenia:

1) Pojazdy budowy przejeżdżające przez główną drogę startową.

c) Ocenić konsekwencje szczegółowych komponentów zagrożeń:

1) Pojazdy budowy mogą odejść od ustalonej procedury i przeciąć/przejechać przez główną drogę startową bez eskorty.

2) Statek powietrzny może znaleźć się w sytuacji konfliktowej z przejeżdżającym pojazdem.

## 4. PROCES OCENIANIA RYZYKA BEZPIECZEŃSTWA

Trzecim zadaniem dla SAG jest identyfikacja i ocena ryzyka bezpieczeństwa konsekwencji zagrożeń i istniejących barier ochronnych, a więc:

a) Ocena przeprowadzona przez SAG prowadzi do wniosku, że istnieje niewielkie prawdopodobieństwo, że pojazdy budowy naruszą ustalone procedury i przetną główną drogę startową bez eskorty.

b) W nocy prowadzone są operacje lotnicze, więc istnieje niewielkie prawdopodobieństwo, że statek powietrzny może znaleźć się w sytuacji konfliktowej z pojazdem.

c) Podczas gdy prawdopodobieństwo konfliktu pomiędzy statkiem powietrznym i pojazdem budowy jest niewielkie, SAG ocenia, że mógłby taki konflikt zaistnieć, a dotkliwość takiego zdarzenia może być katastrofalna.

d) SAG ocenia istniejące bariery ochronne (program szkoleń kierowców, użycie eskorty dla pojazdów budowy, znaki, oznaczenia i oświetlenie).

e) Używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerowalności ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), SAG ocenia ryzyko bezpieczeństwa jako 3A (nieakceptowalne przy istniejących okolicznościach).

f) SAG konkluduje, że ryzyko konsekwencji zagrożeń generowane przez ruch pojazdów budowy na plac budowy, przy panujących okolicznościach, jest nieakceptowalny i konieczna jest kontrola/łagodzenie ryzyka.

## 5. PROCES KONTROLI/ŁAGODZENIA RYZYKA BEZPIECZEŃSTWA

Czwartym i ostatnim zadaniem dla SAG jest złagodzenie ryzyka bezpieczeństwa konsekwencji, a zatem:

a) SAG decyduje, by kontrolować ryzyko konsekwencji zagrożeń, poprzez użycie drogi przy ogrodzeniu do polepszenia dostępu do miejsca budowy. Wszystkie pojazdy budowy będą eskortowane na drodze przy ogrodzeniu.

b) Na podstawie tego łagodzenia ryzyka, SAG ocenił ponownie prawdopodobieństwo wtargnięcia na drogę startową przez pojazd budowy bez eskorty jako skrajnie nieprawdopodobne. Niemniej jednak dotkliwość takiego zdarzenia pozostaje katastrofalna.

c) Użycie drogi przy ogrodzeniu, z powodu powiększonego dystansu do przebycia, może opóźniać pojazdy budowy, ale w ocenie SAG:

1) Podczas gdy to działanie nie usuwa całkowicie możliwości wystąpienia konsekwencji zagrożeń ze zdarzenia (pojazdy budowy ciągle mogą przeciąć drogę startową, z powodu wielości kombinacji okoliczności), niemniej jednak sprowadza to ryzyko konsekwencji (pojazd budowy naruszający ustalone procedury i przejeżdżający przez główną drogę startową bez eskorty; statek powietrzny znajdujący się w sytuacji konfliktowej z pojazdem przejeżdżającym przez drogę startową) do poziomu najniższego z możliwych (ALARP).

d) Używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerowalności ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), SAG ocenia ponownie ryzyko bezpieczeństwa jako 1A (akceptowalne).

e) SAG dokumentuje proces decyzyjny do przyszłego wykorzystania przez Dyrektora ds. Bezpieczeństwa Międzynarodowego Portu Lotniczego w Anycity.

## 6. DZIENNIK IDENTYFIKACJI ZAGROŻEŃ I ZARZĄDANIA RYZYKIEM BEZPIECZEŃSTWA

6.1 Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa z tabeli 5-App 1-1 jest używany do zapewnienia zapisu zidentyfikowanych ryzyk i działań podjętych przez wybrane jednostki (osoby). Zapis powinien być zachowany na stałe w „archiwum bezpieczeństwa” w celu zapewnienia dowodów (śladów) zarządzania ryzykiem bezpieczeństwa i zapewnienia punktu odniesienia dla przyszłych ocen ryzyka bezpieczeństwa.

6.2 Mając zidentyfikowane i uszeregowane ryzyko bezpieczeństwa, każde istniejące przeciwko niemu bariery ochronne powinny być zidentyfikowane. Te bariery muszą być ocenione w kontekście adekwatności. Jeśli te bariery są mniejsze niż powinny być, to podjęte będą dodatkowe czynności. Wszystkie czynności muszą być podjęte przez konkretną osobę (najczęściej odpowiedzialny jest dyrektor) oraz musi zostać wyznaczony czas zakończenia działania. Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa nie może być wymazany przed zakończeniem tych czynności.

**Tabela 5-App 1-1. Identyfikacja zagrożeń i zarządzanie ryzykiem bezpieczeństwa**

| *Rodzaj operacji lub czynności* | *Ogólne zagrożenie* | *Szczegółowe komponenty zagrożenia* | *Konsekwencje związane z zagrożeniem* | *Istniejące bariery ochronne kontrolujące ryzyko oraz indeks ryzyka* | *Dalsze działania zmierzające do redukcji ryzyka i wpływające na indeks ryzyka* |
|---|---|---|---|---|---|
| Operacje na lotnisku | Rozbudowa lotniska | Pojazdy budowy przejeżdżające przez główną drogę startową | a) Pojazdy budowy mogą odejść od ustalonej procedury i przejechać przez główną drogę startową bez eskorty.<br>b) Statek powietrzny może znaleźć się w sytuacji konfliktowej z przejeżdżającym pojazdem. | a) Ocena przeprowadzona przez SAG prowadzi do wniosku, że istnieje niewielkie prawdopodobieństwo, że pojazdy budowy naruszą ustalone procedury i przejadą przez główną drogę startową bez eskorty.<br>b) W nocy prowadzone są operacje lotnicze, więc istnieje niewielkie prawdopodobieństwo, że statek powietrzny może znaleźć się w sytuacji konfliktowej z pojazdem.<br>c) Podczas gdy prawdopodobieństwo konfliktu pomiędzy statkiem powietrznym i pojazdem budowy jest niewielkie, SAG ocenia, że mógłby taki konflikt zaistnieć, a dotkliwość takiego zdarzenia może być katastrofalna.<br>d) SAG ocenia istniejące bariery ochronne (program szkoleń kierowców, użycie eskorty dla pojazdów budowy, znaki, oznaczenia i oświetlenie).<br>e) Używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerowalności ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), SAG ocenia ryzyko bezpieczeństwa jako 3A (nieakceptowalne przy istniejących okolicznościach). | a) SAG decyduje by kontrolować ryzyko konsekwencji zagrożeń poprzez użycie drogi przy ogrodzeniu do polepszenia dostępu do miejsca budowy. Wszystkie pojazdy budowy będą eskortowane na drodze przy ogrodzeniu.<br>b) Na podstawie tego łagodzenia ryzyka, SAG ocenił ponownie prawdopodobieństwo przejechania przez drogę startową przez pojazd budowy bez eskorty jako skrajnie nieprawdopodobne. Niemniej jednak dotkliwość takiego zdarzenia pozostaje katastrofalna.<br>c) Użycie drogi przy ogrodzeniu, z powodu powiększonego dystansu do przebycia, może opóźniać pojazdy budowy, ale w ocenie SAG:<br>1) Podczas gdy to działanie nie usuwa całkowicie możliwości wystąpienia konsekwencji zagrożeń ze zdarzenia (pojazdy budowy ciągle mogą przeciąć drogę startową, z powodu wielości kombinacji okoliczności), niemniej jednak sprowadza to ryzyko konsekwencji (pojazd budowy naruszający ustalone procedury i przejeżdżający przez główną drogę startową bez eskorty); statek powietrzny znajdujący się w sytuacji konfliktowej z pojazdem przejeżdżającym przez drogę startową) do poziomu najniższego z możliwych (ALARP).<br>d) Używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerowalności ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), SAG ocenia ponownie ryzyko bezpieczeństwa jako 1A (akceptowalne).<br>e) SAG dokumentuje proces decyzyjny do przyszłego wykorzystania przez Dyrektora ds. bezpieczeństwa Międzynarodowego Portu Lotniczego w Anycity. |

— — — — — — — — — —

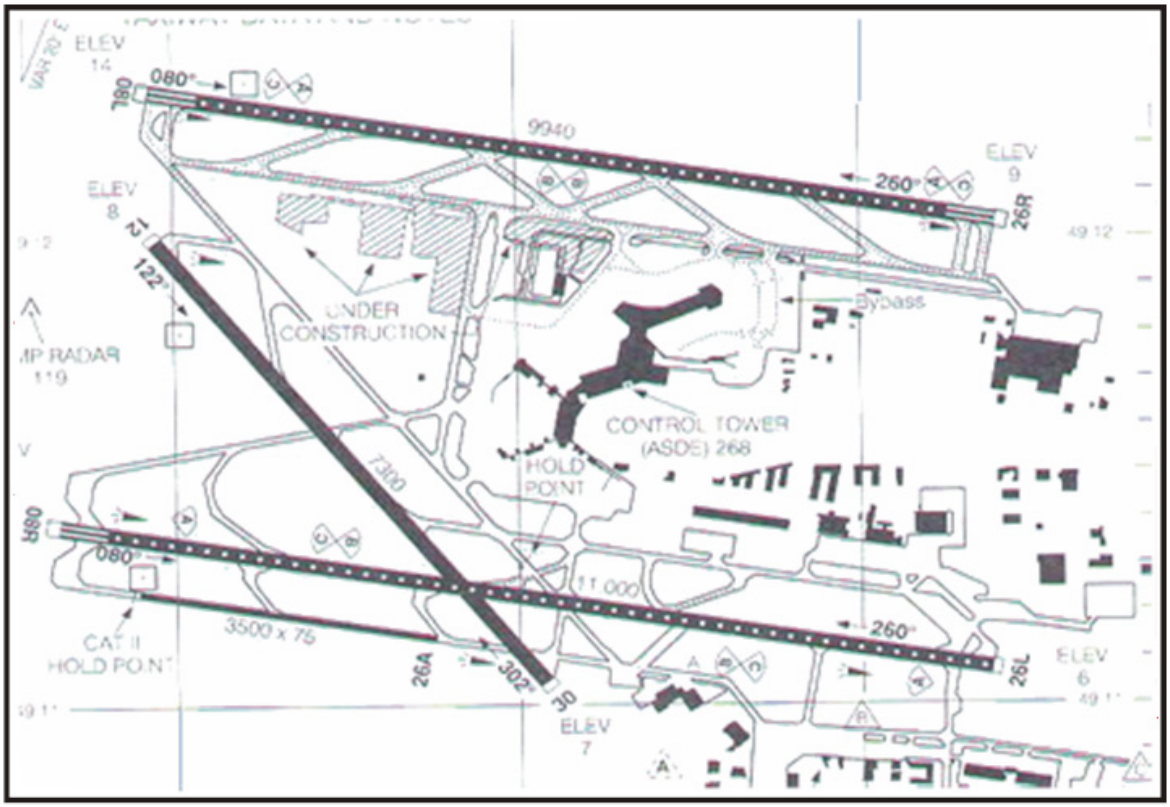
## Dodatek 2 do Rozdziału 5

# OPERACJE NA KRZYŻUJĄCYCH SIĘ DROGACH STARTOWYCH

### 1. SCENARIUSZ

1.1 Organ służby ruchu lotniczego otrzymał informacje od użytkowników portu lotniczego, wyrażające obawy o operacje lotnicze na zbiegających się drogach startowych na lotnisku XYZ. Międzynarodowy Port Lotniczy XYZ posiada trzy drogi startowe 08L/26R, 08R/26L, i 12/30 (zobacz ilustracja 5-App 2-1). Operacje na zbiegających się kierunkach dróg startowych 26R i 12 są przeprowadzane rzadko. Organ kontroli ruchu lotniczego zwrócił się do swojego Dyrektora ds. Bezpieczeństwa o ponowne oszacowanie bezpieczeństwa operacji na zbiegających się kierunkach 26R i 12 w Międzynarodowym Porcie Lotniczym XYZ, pod kątem uwag zgłaszanych przez użytkowników.

1.2 Grupa Reagowania ds. bezpieczeństwa (SAG) została poproszona o wsparcie Dyrektora ds. Bezpieczeństwa organu kontroli ruchu lotniczego w ponownym oszacowaniu bezpieczeństwa operacji na zbiegających się kierunkach 26R i 12 w Międzynarodowym Porcie Lotniczym XYZ. W skład SAG wchodzą przedstawiciele organu kontroli ruchu lotniczego, linii lotniczych operujących na lotnisku, reprezentanci stowarzyszenia pilotów tych linii, przedstawiciele portu lotniczego, jak również przedstawiciele z krajowego podmiotu sprawującego nadzór. Ogólna obawa w zakresie bezpieczeństwa dotyczy zbiegających się tras lotu statków powietrznych startujących i przylatujących na Międzynarodowy Port Lotniczy XYZ. SAG rozpoczyna proces zarządzania ryzykiem bezpieczeństwa w celu ponownego oszacowania bezpieczeństwa operacji na zbiegających się kierunkach dróg startowych.




**Ilustracja 5-App 2-1. Międzynarodowy Port Lotniczy XYZ**

## 2. OPIS SYSTEMU

Jednym z pierwszych zadań SAG jest opisanie systemu, w którym operacje będą przeprowadzane, a więc:

a) Międzynarodowy Port Lotniczy XYZ prowadzi operacje na trzech głównych drogach startowych i małej pomocniczej drodze startowej.

b) Port lotniczy przeprowadza ok. 325 000 operacji rocznie.

c) Droga startowa 26L-08R ma długości 3350 m i jest używana dla wschodnich i zachodnich odlotów i przylotów. Droga startowa 12-30 ma długość 2225 m. Droga startowa 12 jest używana głównie dla przylotów. Droga startowa 30 jest czasem używana dla odlotów i rzadko dla przylotów. Droga startowa 12 fizycznie przecina drogę startową 08R-26L i jest rozważana jako krzyżująca się droga startowa. Droga startowa 08L-26R ma długość 3030 m i jest używana przede wszystkim dla ruchu przylatującego i czasami dla odlatującego. Droga startowa 08L jest używana tylko dla przylotów, ponieważ nie zostały jeszcze ustanowione procedury dla ruchu odlatującego.

d) Oznaczenia, sygnalizacja i oświetlenie portu lotniczego spełnia zarówno standardy organu nadzoru, jak i ICAO.

e) Na wieży używane są dwie częstotliwości radiowe. Jedna częstotliwość jest przeznaczona dla południowych (26L-08R) i zachodnich (12-30) dróg startowych. Druga częstotliwość jest przeznaczona dla północnej drogi startowej (26R-08L).

f) Południowe drogi startowe (26L-08R) mają zbiegające się ścieżki podejścia opublikowane w celu uniknięcia konfliktu z ruchem na drodze startowej 12. Nie ma zbiegających się ścieżek podejścia opublikowanych dla północnych dróg startowych (26R-08L), jako że technicznie nie są one rozpatrywane jako przecinające się, z racji, że fizycznie się nie przecinają. Chociaż droga startowa 12 jest wyposażona w ILS, jest głównie używana jako droga startowa dla ruchu VFR, w którym większość lądowań odbywa się przy podejściu z widocznością.

g) Informacje o ruchu na drodze startowej 12 są obecnie przekazywane razem z informacjami o ruchu na drodze startowej 08R-26L z powodu rozpatrywania tych dróg startowych jako przecinające się. Ruch na obu tych drogach startowych jest kontrolowany przy użyciu tej samej częstotliwości. Jakkolwiek ponieważ drogi startowe 08L-26R i 12 nie przecinają się fizycznie, ruch lotniczy na tych drogach startowych jest kontrolowany przy użyciu różnych częstotliwości. W efekcie informacja o ruchu lotniczym nie jest współdzielona.

h) Pomimo, że separacja ruchu IFR jest zapewniana dla ruchu IFR na drodze 26R, lotniskowe służby kontroli ruchu lotniczego są zapewniane dla ruchu VFR i podejść z widocznością na drogę startową 12. Jakkolwiek kontrolerzy ruchu lotniczego będą podejmować natychmiastowe działania zmierzające do rozwiązania wszelkich zauważonych konfliktów. Standardowa procedura ustala priorytet dla ruchu na drodze startowej 26R-08L i zmian dla ruchu na drodze 12.

## 3. PROCES IDENTYFIKACJI ZAGROŻEŃ

Drugim zadaniem dla SAG jest identyfikacja zagrożeń i ich konsekwencji, które mogą dotknąć operacji lotniczych, jak poniżej:

a) Określenie ogólnego zagrożenia

1) Zbiegające się trasy lotu na drogach startowych 26R-08L i 12, bez względu na to czy statek powietrzny startuje, czy podchodzi do lądowania.

b) Określenie szczegółowego komponentu (szczegółowych komponentów) zagrożenia

1) Statek powietrzny przerywa lądowanie na drodze startowej 26R z powodu statku powietrznego lądującego na drodze startowej 12.

2) Statek powietrzny startuje z drogi startowej 26R naprzeciw statkowi powietrznemu lądującemu na drodze startowej 12.

3) Statek powietrzny podchodzi do lądowania na drodze 08L naprzeciw ruchowi lądującemu na drodze startowej 12.

4) Statek powietrzny wykonuje przejście w bok z podejścia na kierunku 08L na podejście do drogi startowej 08R (lub z drogi 08R na kierunek 08L) będąc w konflikcie z lądującym statkiem powietrznym na drodze 12.

c) Ocena konsekwencji szczegółowych komponentów zagrożenia

1) Napotkanie strug aerodynamicznych.

2) Manewry mające na celu uniknięcie innego statku powietrznego.

3) Utrata kontroli podczas wykonywania manewru unikania innego statku powietrznego.

4) Wypadnięcie z drogi startowej w następstwie niestabilnego podejścia.

5) Zderzenie w powietrzu na przedłużeniu drogi startowej 26R, statku powietrznego podchodzącego do drogi 12 i podchodzącego do drogi startowej 08L lub startującego z drogi 26R (najgorsza możliwość).

## 4. PROCES OCENY RYZYKA BEZPIECZEŃSTWA

4.1 SAG identyfikuje bariery ochronne wspierające operacje na przecinających się kierunkach dróg startowych 26R-08L i 12 w Międzynarodowym Porcie Lotniczym XYZ. Te bariery ochronne przyjmują formę technologii, programów i procedur skierowanych na redukcję ryzyka bezpieczeństwa konsekwencji zbiegających się tras lotu na drogach startowych 26R-08L i 12.

4.2 Bariery zawierają:

a) procedury koordynacji dla kontrolera;

b) zwiększone odstępy w celu zabezpieczenia przestrzeni dla przerwanych podejść w niesprzyjających warunkach pogodowych;

c) ograniczenia przylotów na drogę startową 12, gdy kierunek 26R jest używany dla odlotów;

d) radar obserwacji powierzchni lotniska (aerodrome surface detection equipment - ASDE);

e) program zapobiegania wtargnięciom na drogę startową i program kontroli zwierząt;

f) trening wstępny i odświeżający oraz testy dla kierowców poruszających się po polu manewrowym lotniska;

g) stałe monitorowanie i uzupełnianie statystyk skrajnych wartości bocznych wiatrów;

h) dostępność i użycie radaru podejścia;

i) standardy dla czasów zajmowania drogi startowej;

j) osobne częstotliwości dla wieży;

k) oznaczenia i sygnalizację.

4.3 Bazując na istniejących barierach ochronnych, SAG, używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerancji ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), ocenia ryzyko bezpieczeństwa konsekwencji zbiegających się tras lotu na drogach startowych 26R-08L i 12, jak poniżej:

a) Napotkanie strug aerodynamicznych: prawdopodobieństwo niewielkie, dotkliwość poważna. Tolerancja ryzyka: 3C (akceptowalne bazując na łagodzeniu ryzyka).

b) Manewry mające na celu uniknięcie innego statku powietrznego: prawdopodobieństwo niewielkie, dotkliwość poważna. Tolerancja ryzyka: 3C (akceptowalne bazując na łagodzeniu ryzyka).

c) Utrata kontroli podczas wykonywania manewru unikania innego statku powietrznego: prawdopodobieństwo niewielkie, dotkliwość niebezpieczna. Tolerancja ryzyka: 3B (akceptowalne bazując na łagodzeniu ryzyka).

d) Wypadnięcie z drogi startowej w następstwie niestabilnego podejścia: prawdopodobieństwo niewielkie, dotkliwość niebezpieczna. Tolerancja ryzyka: 3B (akceptowalne bazując na łagodzeniu ryzyka).

e) Zderzenie w powietrzu na przedłużeniu drogi startowej 26R, statku powietrznego podchodzącego do drogi 12 i podchodzącego do drogi startowej 08L lub startującego z drogi 26R: prawdopodobieństwo nieprawdopodobne, dotkliwość katastrofalna. Tolerancja ryzyka: 2A (akceptowalne bazując na łagodzeniu ryzyka).

## 5. PROCES KONTROLI/ŁAGODZENIA RYZYKA BEZPIECZEŃSTWA

5.1 SAG stwierdza, że zakazanie operacji na zbiegających się drogach startowych powinno wyeliminować najgorszą możliwą konsekwencję wynikającą ze zbiegających się tras lotu na drogach startowych 26R-08L i 12: zderzenie w powietrzu na przedłużeniu drogi startowej 26R. Jednakże, działanie wynikające z zarządzania bezpieczeństwem musi być efektywne, a nie tylko skuteczne. Zakaz użycia zbiegających się dróg startowych będzie nieefektywnym rozwiązaniem.

5.2 SAG konkluduje, że nie ma obaw dotyczących bezpieczeństwa, w Międzynarodowym Porcie Lotniczym XYZ, w związku z operacjami na zbiegających się drogach startowych 26R i 12, które wymagają pilnego, natychmiastowego działania. Istniejące bariery ochronne dla ryzyka bezpieczeństwa konsekwencji operacji na przecinających się kierunkach lotu na drogi startowe 26R-08L i 12 w Międzynarodowym Porcie Lotniczym XYZ, włączając w to najgorszy scenariusz (kolizja w powietrzu), skutecznie kontrolują ryzyko bezpieczeństwa by utrzymać je w ALARP (na poziomie najniższym z możliwych). Niemniej jednak zostały opracowane zalecenia zwiększające bezpieczeństwo operacji w Międzynarodowym Porcie Lotniczym XYZ. Chociaż nie są to działania pilne, implementowanie tych zaleceń powinno zapewnić większy margines bezpieczeństwa.

5.3 Rekomendacje zawierają:

a) Zapoczątkowanie stałej kampanii zachęcającej załogi statków powietrznych do wypełniania raportów (pilot reports – PIREPs) dla organu zarządzającego ruchem lotniczym, gdy warunki meteorologiczne odbiegają od prognozy lub oczekiwań.

b) Badanie trafności i efektywności wdrożenia pomocniczego wskaźnika (ekranu) krzyżujących się dróg startowych (converging runway display aid - CRDA), jako niezbędnego urządzenia zwiększającego bezpieczeństwo i przepustowość w Międzynarodowym Porcie Lotniczym XYZ.

c) Jeśli CRDA nie jest wdrożony do użytku w Międzynarodowym Porcie Lotniczym XYZ, ustanowienie kryteriów separacji i procedur dostosowujących odstępy pomiędzy lądującymi statkami powietrznymi, tak, by statek powietrzny przerywający lądowanie na drodze startowej 26R miał zabezpieczoną przestrzeń powietrzną przed statkiem powietrznym, który może podchodzić do drogi startowej 12.

d) Zawarcie na mapach podejść przedziałów ograniczeń prędkości podejścia oraz zmodyfikowanie procedury komunikacji kontrolera ruchu lotniczego, tak, by ruch na drodze startowej 08L-26R był stale informowany o przecinającym się (konfliktowym) ruchu na drodze startowej 12.

e) Zainstalowanie ręcznego przełącznika częstotliwości awaryjnej, tak, by kontroler mógł przełączyć się na częstotliwość innego kontrolera, aby wydać polecenia awaryjne.

5.4 SAG dokumentuje ten proces decyzyjny dla przyszłych uzupełnień z Dyrektorem ds. Bezpieczeństwa organu kontroli ruchu lotniczego.

## 6. DZIENNIK IDENTYFIKACJI ZAGROŻEŃ I ZARZĄDANIA RYZYKIEM BEZPIECZEŃSTWA

6.1 Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa z tabeli 5-App 2-1 jest używany do zapewnienia zapisu zidentyfikowanych ryzyk i działań podjętych przez wybrane jednostki (osoby). Zapis powinien być zachowany na stałe w „archiwum bezpieczeństwa" w celu zapewnienia dowodów (śladów) zarządzania ryzykiem bezpieczeństwa i zapewnienia punktu odniesienia dla przyszłych ocen ryzyka bezpieczeństwa.

6.2 Mając zidentyfikowane i uszeregowane ryzyko bezpieczeństwa, każde istniejące przeciw nim bariery ochronne powinny być zidentyfikowane. Te bariery muszą być ocenione w kontekście adekwatności. Jeśli te bariery są mniejsze niż powinny być, to podjęte będą dodatkowe czynności. Wszystkie czynności muszą zostać podjęte przez konkretną osobę (najczęściej odpowiedzialny jest dyrektor) i musi być wyznaczony czas zakończenia działania. Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa nie może być wymazany przed zakończeniem tych czynności.

**Tabela 5-App 2-1. Identyfikacja zagrożeń i zarządzanie ryzykiem bezpieczeństwa**

| *Rodzaj operacji lub czynności* | *Ogólne zagrożenie* | *Szczegółowe komponenty zagrożenia* | *Konsekwencje związane z zagrożeniem* | *Istniejące bariery ochronne kontrolujące ryzyko oraz indeks ryzyka* | *Dalsze działania zmierzające do redukcji ryzyka i wpływające na indeks ryzyka* |
|---|---|---|---|---|---|
| Działania kontroli ruchu lotniczego | Zbiegając e się trasy lotu na drogach startowych 26R-08L i 12, bez względu na to czy statek powietrzny startuje, czy podchodzi do lądowania. | a) Statek powietrzny przerywa lądowanie na drodze startowej 26R z powodu statku powietrznego lądującego na drodze startowej 12.<br>b) Statek powietrzny startuje z drogi startowej 26R naprzeciw statkowi powietrznem u lądującemu na drodze startowej 12.<br>c) Statek powietrzny podchodzi do lądowania na drodze 08L naprzeciw ruchowi lądującemu na drodze startowej 12.<br>d) Statek powietrzny wykonuje przejście w bok z podejścia na kierunku 08L na podejście do drogi startowej 08R (lub z drogi 08R na kierunek 08L) będąc w konflikcie z lądującym statkiem powietrznym na drodze 12. | a) Napotkanie wirów zaskrzydłowych.<br>b) Manewry mające na celu uniknięcie innego statku powietrznego.<br>c) Utrata kontroli podczas wykonywania manewru unikania innego statku powietrznego.<br>d) Wypadnięcie z drogi startowej w następstwie niestabilnego podejścia.<br>e) Zderzenie w powietrzu na przedłużeniu drogi startowej 26R, statku powietrznego podchodzącego do drogi 12 i podchodzącego do drogi startowej 08L lub startującego z drogi 26R (najgorsza możliwość). | • Procedury koordynacji dla kontrolera;<br>• Zwiększone odstępy w celu zabezpieczenia przestrzeni dla przerwanych podejść w niesprzyjającej pogodzie;<br>• Ograniczenia przylotów na drogę startową 12 gdy kierunek 26R jest używany dla odlotów;<br>• Radar obserwacji powierzchni lotniska (aerodrome surface detection equipment - ASDE);<br>• Program zapobiegania wtargnięciom na drogę startową i program kontroli zwierząt;<br>• Trening wstępny i odświeżający, oraz testy dla kierowców poruszających się po polu manewrowym lotniska;<br>• Stałe monitorowanie i uzupełnianie statystyk skrajnych wartości bocznych wiatrów;<br>• Dostępność i używanie radaru podejścia;<br>• Standardy dla czasów zajmowania drogi startowej;<br>• Osobne częstotliwości dla wieży; oraz<br>• Oznaczenia i sygnalizacja.<br><br>a) Napotkanie wirów zaskrzydłowych:<br>Indeks ryzyka: 3C<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka.<br>b) Manewry mające na celu uniknięcie innego statku powietrznego:<br>Indeks ryzyka: 3C<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka.<br>c) Utrata kontroli podczas wykonywania manewru unikania innego statku powietrznego:<br>Indeks ryzyka: 3B<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka.<br>d) Wypadnięcie z drogi startowej w następstwie niestabilnego podejścia:<br>Indeks ryzyka: 3B<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka.<br>e) Zderzenie w powietrzu na przedłużeniu drogi startowej 26R, statku powietrznego podchodzącego do drogi 12 i podchodzącego do drogi startowej 08L lub startującego z drogi 26R:<br>Indeks ryzyka: 2A<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka. | a) Zapoczątkowanie stałej kampanii zachęcającej załogi statków powietrznych do wypełniania raportów (pilot reports – PIREPs) dla organu zarządzającego ruchem lotniczym, gdy warunki meteorologiczne odbiegają od prognozy lub oczekiwań.<br>b) Badanie trafności i efektywności wdrożenia CRDA, jako niezbędnego urządzenia zwiększającego bezpieczeństwo i przepustowość w Międzynarodowym Porcie Lotniczym XYZ.<br>c) Jeśli CRDA nie jest wdrożony do użytku w Międzynarodowym Porcie Lotniczym XYZ, ustanowienie kryteriów separacji i procedur dostosowujących odstępy pomiędzy lądującymi statkami powietrznymi, tak by statek powietrzny przerywający lądowanie na drodze startowej 26R miał zabezpieczoną przestrzeń powietrzną przed statkiem powietrznym, który może podchodzić do drogi startowej 12.<br>d) Umieszczenie na mapach podejść przedziałów ograniczeń prędkości podejścia, oraz zmodyfikowanie procedury komunikacji kontrolera ruchu lotniczego, tak by ruch na drodze startowej 08L-26R był stale informowany o przecinającym się (konfliktowym) ruchu na drodze startowej 12.<br>e) Zainstalowanie ręcznego przełącznika częstotliwości awaryjnej, tak by kontroler mógł przełączyć się na częstotliwość innego kontrolera by wydać polecenia awaryjne polecenia. |

## Dodatek 3 do Rozdziału 5

# OPERACJE KOMERCYJNE W MIĘDZYNARODOWYM PORCIE LOTNICZYM ANDES CITY

### 1. SCENARIUSZ

1.1 Linie Lotnicze "*Safe Airways*" to średniej wielkości operator lotniczy operujący flotą piętnastu nowoczesnych, dwusilnikowych odrzutowców. Linia planuje rozpocząć komercyjne loty do Andes City, które jest kurortem położonym w wysokich górach, otoczonym pięknym widokiem i z pozostałościami starożytnej cywilizacji. Transport drogą lądową, po niebezpiecznych drogach, może trwać ponad dwa dni, dlatego transport lotniczy jest najlepszym środkiem transportu.

1.2 Andes City jest obsługiwane przez wysoko położone lotnisko, ze skomplikowanym otoczeniem geograficznym, bez pomocy nawigacyjnych, co skutkuje ograniczeniem operacji lotniczych do pory dziennej i warunków VMC. Wyższe kierownictwo *Safe Airways* zażądało, by dyrektor ds. operacji lotniczych wdrożył operacje spełniające wszystkie wymogi bezpieczeństwa i jednocześnie zapewnił maksymalne załadowanie statków powietrznych z zachowaniem ich osiągów i limitów. Planowana operacja powinna zawierać wczesno popołudniowy lot do Andes City z szybkim powrotem do głównej bazy operatora, oddalonej o dziewięćdziesiąt minut lotu.

1.3 Dyrektor ds. operacji lotniczych prosi Dyrektora ds. bezpieczeństwa, wspieranego przez Grupę Reagowania ds. Bezpieczeństwa (SAG), by oszacował konsekwencje dla bezpieczeństwa operacji do Międzynarodowego Portu Lotniczego w Andes City. Najpilniejszym i oczywiście ogólnym obszarem rozważań są operacje na wysoko położone lotnisko, ze skomplikowanym otoczeniem geograficznym, bez pomocy nawigacyjnych. SAG rozpoczyna proces zarządzania ryzykiem bezpieczeństwa w celu ponownego oszacowania konsekwencji dla bezpieczeństwa operacji w Andes City.

### 2. OPIS SYSTEMU

Jednym z pierwszych zadań dla SAG jest opisanie systemu, w którym będą prowadzone operacje, a więc:

a) Międzynarodowy Port Lotniczy w Andes City jest położony w dolinie, na wysokości 3350 m (11000 ft), otoczonej górami o wysokości ponad 4870 m (16000 ft).

b) Lotnisko posiada tylko jedną drogę startową o długości 3400 m (11155 ft), o kierunku wschód-zachód (09-27).

c) Z powodu topografii terenu, droga startowa 09 używana jest wyłącznie do lądowania, a droga 27 wyłącznie do startu.

d) W odległości 37 km (20 NM) na zachód od lotniska, w dolinie, zlokalizowany jest VOR, używany do instrumentalnego podejścia ze zniżaniem (instrument letdown approach).

e) Nie jest dostępny ILS.

f) Nie jest wydawana zgoda na podejście z widocznością od momentu wydania załodze odlatującego statku powietrznego zgody na start, do momentu zgłoszenia przez załogę tego statku, osiągnięcia wysokości przelotowej ponad przeszkodami.

g) Podejścia VMC do lądowania w Andes City rozpoczyna się na 18000 ft, nad VOR. Jeśli na wysokości 18000 ft załoga nie ma kontaktu wzrokowego z ziemią podejście nie jest autoryzowane przez ATC.

h) Nie są dostępne wzrokowe pomoce lądowania.

i) Nie jest wydawana zgoda na start dopóki statek powietrzny, którego załoga otrzymała zgodę na podejście z widocznością do Międzynarodowego Portu Lotniczego w Andes City, nie wyląduje i załoga nie zgłosi opuszczenia drogi startowej po lądowaniu.

j) Pogoda w Andes City jest zmienna, często występują wysokie warstwy chmur o podstawie ok. 5700 – 6400 m (19000 – 21000 ft).

k) W godzinach 10:00 – 14:00 temperatura powietrza jest wysoka, co ma negatywny wpływ na osiągi statków powietrznych.

l) Po godzinie 16:00 wiatry katabatyczne mogą wymuszać konieczność startów z tylnym wiatrem, z kierunku 27.

m) W przypadku wystąpienia pożaru lub wyłączenia silnika albo jakiejkolwiek sytuacji awaryjnej, powrót na lotnisko jest obowiązkowy, jako że masa i ograniczenia osiągowe sprawiłyby, iż spełnienie wymaganego przewyższenia nad przeszkodami i utrzymanie się w sieci dróg byłoby mało prawdopodobne.

n) Krajowe władze lotnictwa cywilnego (CAA) do uzyskania pozwolenia na operacje specjalne, będącego częścią uprawnień operatora, wymagają, by linia lotnicza zademonstrowała, że statek powietrzny może utrzymać się w siatce przebiegu dróg i zachować separację od przeszkód w fazach podejścia do lądowania, startu, wznoszenia i przelotu oraz że może manewrować w skomplikowanym otoczeniu geograficznym, mieszcząc się w marginesie bezpieczeństwa i ograniczeniach statku powietrznego.

o) Lot testowy jest wymagany przez CAA, gdy operacja jest gotowa do wdrożenia, po przejrzeniu i zatwierdzeniu dokumentacji oraz po przeszkoleniu załogi i personelu pokładowego z zakresu operowania na Międzynarodowym Porcie Lotniczym w Andes City.

### 3. PROCES IDENTYFIKACJI ZAGROŻEŃ

Drugim zadaniem dla SAG, jest identyfikacja zagrożeń, które mogą dotknąć operacje prowadzone w Międzynarodowym Porcie Lotniczym w Andes City i ich konsekwencji, a więc:

a) Określenie ogólnego zagrożenia

   1) Operacje na wysoko położonym lotnisku ze skomplikowanym otoczeniem geograficznym.

b) Określenie szczegółowych komponentów zagrożenia

   1) Górzyste otoczenie.

   2) Wysokie położenie lotniska.

   3) Brak pomocy nawigacyjnych do podejścia i lądowania.

   4) Brak wzrokowych pomocy do lądowania.

   5) Konfliktowy ruch lotniczy.

   6) Śliska droga startowa (gdy jest mokra).

   7) Dzikie zwierzęta.

c) Ocena konsekwencji szczegółowych komponentów ogólnego zagrożenia

1) Kontrolowane zderzenie z terenem (*Controlled Flight Into Terrain CFIT*), spowodowane:

I) Utratą krytycznego silnika w czasie podejścia i lądowania;

II) Utratą krytycznego silnika w czasie startu, powyżej V1;

III) Utratą krytycznego silnika w czasie wznoszenia.

2) Kolizja w powietrzu.

3) Wypadnięcie z pasa podczas lądowania.

4) Wypadnięcie z pasa podczas przerwanego startu.

5) Zderzenie z ptakami.

## 4. PROCES OCENY RYZYKA BEZPIECZEŃSTWA

*Uwaga.— Kontrolowane zderzenie z terenem* (*Controlled Flight Into Terrain CFIT*) *z powodu awarii krytycznego silnika w czasie startu, po przekroczeniu V1 jest jedyną konsekwencją analizowaną w tym ćwiczeniu. W rzeczywistym procesie oceny ryzyka bezpieczeństwa wszystkie konsekwencje muszą być przeanalizowane, wszystkie ryzyka bezpieczeństwa muszą być ocenione i złagodzone.*

4.1 Trzecim zadaniem dla SAG jest ocenienie efektywności istniejących barier ochronnych dla ryzyka bezpieczeństwa konsekwencji zagrożeń.

4.2 SAG dokonuje przeglądu istniejących barier ochronnych, które mogą być dotknięte lub brakuje ich w relacji do tej operacji. Te bariery ochronne odwołują się głównie do treningu załóg, procedur i ograniczeń w instrukcji operacyjnej przedsiębiorstwa, w relacji do podobnych operacji.

4.3 Istniejące bariery ochronne, zidentyfikowane w czasie oceny, to:

a) operacje lotnicze tylko w warunkach VMC i w dzień;

b) opis lotniska dostępny w krajowym AIP;

c) wprowadzone na lotnisku procedury ATC;

d) instrukcja operacyjna przedsiębiorstwa;

e) instrukcja parametrów spedycyjnych;

f) instrukcja użytkowania statku powietrznego;

g) szkolenia odświeżające z tematyki awarii silnika przed i po osiągnięciu V1 oraz procedury nieudanego podejścia;

h) szkolenia CRM.

4.4 SAG uznał istniejące bariery jako nieodpowiednie, głównie z powodu, że nie zajmują się określoną operacją na wysoko położone lotnisko ze skomplikowanym otoczeniem geograficznym.

4.5 Dokumentacja operacyjna i obowiązujące procedury ATC na lotnisku w Andes City jest poddana analizie.

4.6 Używając macierzy oceny ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-4) i macierzy tolerancji ryzyka bezpieczeństwa (rozdział 5, ilustracja 5-5), SAG ocenia indeks ryzyka bezpieczeństwa jako 3A (nieakceptowalne przy istniejących okolicznościach).

## 5. PROCES KONTROLI/ŁAGODZENIA RYZYKA BEZPIECZEŃSTWA

5.1 Czwartym i ostatnim zadaniem dla SAG jest kontrolowanie i łagodzenie zidentyfikowanych ryzyk dla bezpieczeństwa konsekwencji CFIT z powodu utraty krytycznego silnika w czasie startu, po osiągnięciu V1. Po kilku spotkaniach SAG zaproponował kilka sposobów łagodzenia ryzyka. Zaproponowane działania łagodzące są skierowane na wzmocnienie barier ochronnych i zmniejszenie ryzyka bezpieczeństwa do poziomu najniższego z możliwych (ALARP). Działania łagodzące obejmują:

a) Opracowanie procedur startu i wznoszenia na wypadek utraty krytycznego silnika po osiągnięciu V1, które rozważałyby możliwość powrotu i lądowania.

b) Opracowanie i zapewnienie treningu w ramach powyższych procedur (pełne szkolenie symulatorowe i odnawianie kwalifikacji co sześć miesięcy).

c) Rozważenie, czy Międzynarodowy Port Lotniczy w Andes City nie powinien być “lotniskiem specjalnym”, które wymaga specjalnych kwalifikacji załogi odnawianych co roku.

d) Zapewnienie właściwych szkoleń dla załóg kabinowych, z zakresu operowania na „lotnisko specjalne”. (To łagodzenie nie jest skierowane na prawdopodobieństwo, ale na dotkliwość [ewakuacja] ryzyka bezpieczeństwa.)

e) Zapewnienie precyzyjnych informacji meteorologicznych, zwłaszcza wiatrów przyziemnych po godzinie 16:00.

f) Rozwinięcie dokumentacji operacyjnej poprzez zawarcie zapisów w instrukcji operacyjnej przedsiębiorstwa i podręcznik spedytora do zatwierdzenia przez CAA.

g) Zakaz stosowania listy minimalnego wyposażenia (MEL) dla krytycznych elementów.

h) W ramach programu poprawy solidności obsługi technicznej, dział obsługi technicznej zwróci szczególną uwagę na silniki statku powietrznego przygotowywanego do startu.

i) Kontrolowanie środków bezpieczeństwa i nowych barier ochronnych zaimplementowanych dla kontroli i łagodzenia ryzyka bezpieczeństwa, w odniesieniu do operacji w Międzynarodowym Porcie Lotniczym w Andes City. Przegląd efektywności barier jest planowany po sześciu i po dwunastu miesiącach po wprowadzeniu zmian i zatwierdzeniu ich przez CAA.

5.2 Biorąc pod uwagę nowe bariery ochronne wprowadzone dla tych specjalnych operacji, ryzyko CFIT z powodu utraty krytycznego silnika podczas startu, po osiągnięciu V1 jest obecnie ocenione jako nieprawdopodobne (2 – mało prawdopodobne, że wystąpi), chociaż dotkliwość CFIT ciągle pozostaje katastrofalna (A — zniszczony sprzęt, wiele ofiar).

5.3 Operacja obecnie trafia w tolerowany rejon, a osiągnięty indeks ryzyka to 2A (akceptowalne na podstawie łagodzenia ryzyka). Może to wymagać decyzji odnoszących się do zarządzania (zobacz rozdział 5, ilustracja 5-8). Dane i dokumentacja zebrana podczas procesu identyfikacji zagrożeń i procesu zarządzania ryzykiem są włączone do „archiwum bezpieczeństwa”.

## 6. INDYWIDUALNA ODPOWIEDZIALNOŚĆ ZA IMPLEMENTOWANE ŚRODKI ŁAGODZĄCE RYZYKO

Indywidualna odpowiedzialność za implementację zaproponowanych środków przedstawia się następująco:

a) Środki łagodzące ryzyko a), f) oraz i) — Dyrektor ds. operacji lotniczych;

b) Środki łagodzące ryzyko b), c) oraz d) — Dyrektor ds. szkolenia w locie;

c) Środek łagodzący ryzyko e) — Dyrektor ds. spedycji;

d) Środki łagodzące ryzyko g) oraz h) — Dyrektor ds. obsługi technicznej.

## 7. DZIENNIK IDENTYFIKACJI ZAGROŻEŃ I ZARZĄDANIA RYZYKIEM BEZPIECZEŃSTWA

7.1 Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa z tabeli 5-App 2-1 jest używany do zapewnienia zapisu zidentyfikowanych ryzyk i działań podjętych przez wybrane jednostki (osoby). Zapis powinien być zachowany na stałe w „archiwum bezpieczeństwa” w celu zapewnienia dowodów (śladów) zarządzania ryzykiem bezpieczeństwa i zapewnienia punktu odniesienia dla przyszłych ocen ryzyka bezpieczeństwa.

7.2 Mając zidentyfikowane i uszeregowane ryzyko bezpieczeństwa, każde istniejące przeciw nim bariery ochronne powinny być zidentyfikowane. Te bariery muszą być ocenione w kontekście adekwatności. Jeśli te bariery są mniejsze niż powinny być, to podjęte będą dodatkowe czynności. Wszystkie czynności muszą być podjęte przez konkretną osobę (najczęściej odpowiedzialny jest dyrektor) i musi być wyznaczony czas zakończenia działania. Dziennik identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa nie może być wymazany przed zakończeniem tych czynności.

**Tabela 5-App 3-1. Identyfikacja zagrożeń i zarządzanie ryzykiem bezpieczeństwa**

| *Rodzaj operacji lub czynności* | *Ogólne zagrożenie* | *Szczegółowe komponenty zagrożenia* | *Konsekwencje związane z zagrożeniem* | *Istniejące bariery ochronne kontrolujące ryzyko oraz indeks ryzyka* | *Dalsze działania zmierzające do redukcji ryzyka i wpływające na indeks ryzyka* | *Osoba odpowiedzialna* |
|---|---|---|---|---|---|---|
| Operacje lotnicze. | Operacje na wysoko położonym lotnisku, ze skomplikowanym otoczeniem geograficznym. | a) Górzyste otoczenie.<br>b) Wysokie położenie lotniska.<br>c) Brak pomocy nawigacyjnych do podejścia i lądowania.<br>d) Brak wzrokowych pomocy do lądowania.<br>e) Konfliktowy ruch lotniczy.<br>f) Śliska droga startowa (gdy jest mokra).<br>g) Zwierzęta. | a) Kontrolowane zderzenie z terenem (CFIT), spowodowane:<br>1. Utratą krytycznego silnika w czasie podejścia i lądowania;<br>2. Utratą krytycznego silnika w czasie startu, powyżej V1;<br>3. Utratą krytycznego silnika w czasie wznoszenia.<br>b) Kolizja w powietrzu.<br>c) Wypadnięcie z pasa podczas lądowania.<br>d) Wypadnięcie z pasa podczas przerwanego startu.<br>e) Zderzenie z ptakiem. | a) Operacje lotnicze tylko w warunkach VMC i tylko w dzień;<br>b) Opis lotniska dostępny w krajowym AIP;<br>c) Wprowadzone na lotnisku procedury ATC;<br>d) Instrukcja operacyjna operatora;<br>e) Instrukcja parametrów spedycyjnych;<br>f) Instrukcja użytkowania statków powietrznych;<br>g) Szkolenia odświeżające z awarii silnika przed i po V1, oraz procedury nieudanego podejścia;<br>h) Szkolenie CRM.<br>Indeks ryzyka: 3A, ryzyko bezpieczeństwa tolerowalne: nieakceptowane w istniejących okolicznościach. | a) Opracowanie procedur startu i wznoszenia na wypadek utraty krytycznego silnika po V1, możliwość powrotu do lądowania.<br>b) Opracowanie i zapewnienie treningu w ramach powyższych procedur (pełne szkolenie symulatorowe i odnawianie kwalifikacji co sześć miesięcy).<br>c) Rozważenie, czy Międzynarodowy Port Lotniczy w Andes City nie powinien być "lotniskiem specjalnym", które wymaga specjalnych kwalifikacji załogi odnawianych co roku.<br>d) Zapewnienie właściwych szkoleń dla załóg kabinowych, z zakresu operowania na „lotnisko specjalne". (To łagodzenie nie jest skierowane na prawdopodobieństwo, ale na dotkliwość [ewakuacja] ryzyka bezpieczeństwa.)<br>e) Zapewnienie precyzyjnych informacji meteorologicznych, zwłaszcza wiatrów przyziemnych po godzinie 16:00.<br>f) Rozwinięcie dokumentacji operacyjnej poprzez zawarcie zapisów w instrukcji operacyjnej przedsiębiorstwa i podręcznik spedytora, do zatwierdzenia przez CAA. | Dyrektor ds. operacji lotniczych<br>Dyrektor ds. szkolenia<br>Dyrektor ds. szkolenia<br>Dyrektor ds. szkolenia<br>Kierownik ds. wyważenia i osiągów<br>Dyrektor ds. operacji lotniczych |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | g) Zakaz stosowania listy minimalnego wyposażenia (MEL) dla krytycznych elementów. | Dyrektor ds. obsługi technicznej |
| | | | | | h) W ramach programu poprawy solidności obsługi technicznej, dział obsługi technicznej zwróci szczególną uwagę na silniki statku powietrznego przygotowywanego do startu. | Dyrektor ds. obsługi technicznej |
| | | | | | i) Kontrolowanie środków bezpieczeństwa i nowych barier ochronnych zaimplemento-wanych dla kontroli i łagodzenia ryzyka bezpieczeństwa, w odniesieniu do operacji w Międzynarodowym Porcie Lotniczym w Andes City. Przegląd efektywności barier jest planowany po sześciu i po dwunastu miesiącach po wprowadzeniu zmian i zatwierdzeniu ich przez CAA.<br>Tolerancja ryzyka: akceptowalne bazując na łagodzeniu ryzyka. Może wymagać decyzji Zarządu. | Dyrektor ds. operacji lotniczych |

# Rozdział 6

# WYMAGANIA ICAO DOTYCZĄCE ZARZĄDZANIA BEZPIECZEŃSTWEM

## 6.1 CEL I ZAWARTOŚĆ

W tym rozdziale przedstawiono normy oraz zalecane metody i zasady postępowania w zakresie zarządzania bezpieczeństwem ustanowione przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO). Znajdują się one w Załączniku 1 – *Licencjonowanie Personelu*, Załączniku 6 – *Eksploatacja statków powietrznych,* Załączniku 8 – *Zdatność do lotu statków powietrznych*, Załączniku 11 – *Służby ruchu lotniczego*, Załączniku 13 – *Badanie wypadków i incydentów statków powietrznych* oraz w Załączniku 14 – *Lotniska.* W niniejszym rozdziale przedstawiono także istniejące zależności pomiędzy Krajowym programem bezpieczeństwa (*State Safety Programme - SSP*) a systemem zarządzania bezpieczeństwem dostawców usług (*Safety Management System - SMS*).
Rozdział ten omawia następujące zagadnienia:

a) Normy oraz zalecane metody i zasady postępowania (SARPs) w zarządzaniu bezpieczeństwem Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) – Uwagi ogólne;

b) Krajowy program bezpieczeństwa (SSP);

c) Akceptowalny lub inaczej dopuszczalny poziom bezpieczeństwa *(Acceptable Level of Safety – ALoS*);

d) System zarządzania bezpieczeństwem (*Safety Management System -SMS*);

e) Efektywność SMS;

f) Odpowiedzialność kierownictwa;

g) Zależności pomiędzy krajowym programem bezpieczeństwa (SSP) a systemem zarządzania bezpieczeństwem (SMS);

h) Zgodność (z przepisami) i efektywność.

## 6.2 ZARZĄDZANIE BEZPIECZEŃSTWEM WEDŁUG SARPs ICAO – UWAGI OGÓLNE

6.2.1 Międzynarodowe normy oraz zalecane metody i zasady postępowania (SARPs) Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) w zakresie zarządzania bezpieczeństwem są zawarte w Załącznikach 1; 6; Część I i III; 8; 11; 13 oraz 14. Załączniki te odnoszą się do działalności prowadzonej przez zatwierdzone organizacje szkoleniowe, międzynarodowych operatorów statków powietrznych, zatwierdzone organizacje obsługi technicznej, organizacje odpowiedzialne za projekty typu i/lub produkcję statków powietrznych, organizacje zapewniające obsługę ruchu lotniczego i certyfikowane lotniska. W przypadku Załącznika 1, normy oraz zalecane metody i zasady postępowania ICAO w obszarze zarządzania bezpieczeństwem ograniczone zostały wyłącznie do zatwierdzonych organizacji szkoleniowych, w przypadku których występują zagrożenia bezpieczeństwa na etapie świadczenia usług.

6.2.2 Normy oraz zalecane metody i zasady postępowania SARPs w zakresie zarządzania bezpieczeństwem skierowane są do dwóch grup odbiorców: Państw oraz dostawców usług świadczących usługi. W tym podręczniku termin „dostawca usług" stosowany jest do każdej organizacji, świadczącej usługi w dziedzinie lotnictwa. Tym samym określenie to obejmuje zatwierdzone organizacje szkoleniowe, które są narażone na wystąpienie zagrożenia bezpieczeństwa w trakcie świadczenia usług, operatorów statków powietrznych, zatwierdzone organizacje obsługi technicznej, organizacje odpowiedzialne za projekty typu i/lub produkcję statków powietrznych, organizacje zapewniające obsługę ruchu lotniczego i certyfikowane lotniska, jeśli dotyczy.

6.2.3 Normy oraz zalecane metody i zasady postępowania SARPs w zarządzaniu bezpieczeństwem odnoszą się do trzech różnych wymagań:

a) wymagań dotyczących Krajowego programu bezpieczeństwa (SSP), w tym akceptowalnego poziomu bezpieczeństwa (*ALoS*) zdefiniowanego w ramach SSP;

b) wymagań dotyczących systemów zarządzania bezpieczeństwem (SMS), w tym efektywności SMS;

c) wymagań dotyczących odpowiedzialności kierownictwa w kontekście zarządzania bezpieczeństwem w trakcie świadczenia usług.

6.2.4 Normy oraz zalecane metody i zasady postępowania SARPs w zarządzaniu bezpieczeństwem wprowadzają pojęcie dopuszczalnego poziomu bezpieczeństwa jako sposobu wyrażania minimalnego poziomu bezpieczeństwa, które zostało ustanowione przez państwo i musi być zapewnione poprzez SSP oraz pojęcie efektywności bezpieczeństwa (*safety performance)* jako sposobu pomiaru stopnia realizacji założeń i działań na rzecz bezpieczeństwa, podejmowanych przez dostawców usług, świadczących usługi lotnicze oraz efektywności funkcjonowania jego SMS.

### 6.3 KRAJOWY PROGRAM BEZPIECZEŃSTWA (SSP)

6.3.1 Załączniki 1, 6, 8, 11, 13 i 14 zawierają wymóg, nakładający na państwo obowiązek ustanowienia krajowego programu bezpieczeństwa (SSP), w celu osiągnięcia akceptowalnego poziomu bezpieczeństwa w lotnictwie cywilnym. SSP stanowi system zarządzania, przy pomocy którego państwo zarządza bezpieczeństwem.

6.3.2 SSP jest zdefiniowany jako zintegrowany zestaw przepisów i działań mających na celu poprawę bezpieczeństwa. Zawiera on konkretne działania w zakresie bezpieczeństwa, które muszą zostać podjęte przez państwo, jak również rozporządzenia i dyrektywy wydawane przez państwo, w celu wsparcia realizacji jego obowiązków dotyczących bezpieczeństwa i skutecznej realizacji działań oraz funkcji lotniczych w Państwie.

6.3.3 Aby pomóc państwom w budowaniu ich SSP, Organizacja Międzynarodowego Lotnictwa Cywilnego nakreśliła pewne ramy koncepcyjne, obejmujące poszczególne składniki i elementy SSP. Wspomniana struktura SSP składa się z czterech części i jedenastu elementów i w całości została przedstawiona w Rozdziale 11. Obowiązki określone w SSP nie są zupełną nowością. Należy oczekiwać, co jest uzasadnione, że większość państw wypełnia większość tych obowiązków. Nowością jest pojęcie SSP samo w sobie, sugerujące jeden sposób zorganizowania i przydzielenia zadań w zakresie odpowiedzialności i obowiązków państwa w zakresie bezpieczeństwa według ustalonych zasad i w sposób uporządkowany. Nowością jest również ocena skuteczności, z jaką państwo wywiązuje się z odpowiedzialności za bezpieczeństwo oraz z jaką wypełnia swoje obowiązki na rzecz bezpieczeństwa. Organizacja zadań w zakresie bezpieczeństwa państwa ma na celu śledzenie przestrzegania pewnych zasad i standardowej struktury, kierowana jest na działania mające na celu podwyższanie bezpieczeństwa jako udokumentowane, precyzyjne i możliwe do prześledzenia. Podczas gdy długoterminowym, strategicznym celem SSP jest poprawa bezpieczeństwa w państwie, zorganizowanie SSP ma dwa krótkoterminowe cele taktyczne: skuteczne i efektywne zapewnienie bezpieczeństwa przez państwo i skuteczne monitorowanie realizacji zadań w zakresie bezpieczeństwa państwa.

6.3.4 Nie należy lekceważyć znaczenia drugiego celu, jakim jest skuteczne nadzorowanie realizacji zadań i odpowiedzialności państwa w zakresie bezpieczeństwa. W chwili obecnej ICAO, w ramach programu obejmującego audyty nadzoru nad bezpieczeństwem w państwach (*Universal State Oversight Audit Programme – USOAP)*, w sposób kompleksowy monitoruje zadania państwa w zakresie bezpieczeństwa, co zostało określone i ustanowione w Załącznikach do Konwencji o Międzynarodowym Lotnictwie Cywilnym. Zdefiniowane zostały krytyczne elementy, które muszą być monitorowane przez państwowy system nadzoru, zaś audyt USOAP pozwala zweryfikować stan wdrożenia poszczególnych elementów i funkcji, wskazując na zgodność, bądź brak zgodności z określonymi wymaganiami. Przewiduje się, że gdy koncepcja SSP osiągnie dojrzałość i będzie stosowana we wszystkich państwach, program audytowy USOAP będzie nadzorować SSP w sposób bardziej całościowy, aniżeli elementy funkcji nadzoru nad bezpieczeństwem, poprzez podejście oparte na koncepcji ciągłego monitorowania.

6.3.5 Koncepcja SSP ma również trzeci, średniookresowy cel: przejście od systemu opartego na sztywnych normach i nakazach (*prescriptive-based approach*) do zintegrowanego systemu regulacyjnego, łączącego podejście oparte na normach i nakazach z podejściem opartym na działaniach i wynikach działań (*performance-based approach*). W tym przejściowym przechodzeniu z jednego systemu do drugiego fundamentalne znaczenie ma, omawiane w dalszej części tego rozdziału, pojęcie akceptowalnego poziomu bezpieczeństwa (*ALoS*), określonego w SSP oraz pojęcie poziomu bezpieczeństwa, będącego efektem funkcjonowania SMS (*safety performance*), które to obydwa pojęcia tworzą komponent zapewnienia bezpieczeństwa (*safety assurances*) zarówno w ramach SSP, jak i systemu zarządzania bezpieczeństwem. Ta przemiana jednak musi rozpocząć się od jasnego ustalenia roli, jaką ma pełnić nadzór państwowy w zakresie kontroli bezpieczeństwa w ramach SSP oraz ich wzajemnych relacji.

6.3.6 Funkcja nadzoru nad bezpieczeństwem Państwa jest częścią SSP i podstawą komponentu zapewnienia bezpieczeństwa. Cele funkcji bezpieczeństwa nadzoru państwa w tradycyjnej praktyce są wypełniane poprzez kontrole administracyjne (inspekcje, audyty i przeglądy), regularnie przeprowadzane przez władze lotnictwa cywilnego i niekoniecznie spełniają funkcję kontroli ryzyka zagrożeń dla bezpieczeństwa, jak to opisano w rozdziale 5 oraz w podrozdziale 6.8. SSP jest niezbędny, aby wyniki nadzoru nad bezpieczeństwem przełożyć na kontrolę ryzyka zagrażającego bezpieczeństwu. Dla przykładu obecnie funkcja nadzoru państwa nad bezpieczeństwem weryfikuje, czy państwo posiada system regulacji, ale nie wymaga analizy ryzyka zagrażającego bezpieczeństwu na etapie ustanawiania takich przepisów, jak również nie monitoruje skuteczności rozporządzeń co do kontroli ryzyka bezpieczeństwa. Z drugiej strony, SSP uwzględnia ocenę ryzyka i poprzez element zarządzania ryzykiem wymaga, by w procesie stanowienia prawa uwzględniać zasady zarządzania ryzykiem dla bezpieczeństwa (identyfikacja zagrożeń, ocena ryzyka wystąpienia konsekwencji zagrożeń dla bezpieczeństwa, a także tworzenie przepisów, które przewidują dopuszczalne ograniczenie/kontrola skutków zagrożeń). W drugim etapie, poprzez komponent zapewnienia bezpieczeństwa, SSP monitoruje efektywność i wydajność regulacji w zakresie kontroli ryzyka zagrożenia dla bezpieczeństwa.

6.3.7 Wyraźne określenie różnicy pomiędzy regulacjami jako formą kontroli administracyjnej a regulacjami jako kontrolą oceny ryzyka, wskazuje na odejście od regulacji o formie nakazowej w kierunku regulacji opartej na realizacji i efektywności działań. SSP w wersji zaproponowanej w Rozdziale 11 jest pierwszym krokiem umożliwiającym taką zmianę podejścia. Ponadto integracja z SSP, tam gdzie jest to wskazane, zasad podkreślających rolę krytycznych elementów funkcji państwowego nadzoru bezpieczeństwa pozwoli w efekcie na stworzenie bardziej wydajnego i skutecznego SSP.

### 6.4 AKCEPTOWALNY POZIOM BEZPIECZEŃSTWA (Acceptable Level of Safety - ALoS)

6.4.1 Załączniki 1, 6, 8, 11, 13 i 14 wymagają, aby akceptowalny (dopuszczalny) poziom bezpieczeństwa (ALoS) jaki ma być osiągnięty (przez SSP), został ustalony przez państwo.

6.4.2 Pojęcie akceptowalnego poziomu bezpieczeństwa stanowi istotny element efektywnego funkcjonowania SSP. Jeśli pojęcie akceptowalnego poziomu bezpieczeństwa nie zostanie zrozumiane i dobrze zdefiniowane, a następnie wdrożone, trudno będzie stworzyć oparte na realizacji założeń i efektywności działań środowisko regulacyjne, a także monitorować rzeczywistą skuteczność SSP. Funkcjonowanie SSP może zostać sprowadzone do wykonywania prostych, mechanicznych czynności polegających na zaznaczeniu odpowiedniego pola na arkuszu uzgodnień, pod pretekstem realizacji funkcji zarządzania bezpieczeństwem.

6.4.3 Podstawowy aforyzm, że „nie można zarządzać tym, czego się nie zmierzy," został omówiony w innej części niniejszego podręcznika. W każdym systemie konieczne jest opracowanie zbioru mierzalnych wyników działalności, aby móc wykazać, czy system rzeczywiście pracuje zgodnie z oczekiwanymi założeniami, aniżeli tylko funkcjonuje zgodnie z określonymi wymaganiami regulacyjnymi. Zdefiniowanie zestawu mierzalnych rezultatów działalności pozwala także stwierdzić, w którym miejscu zachodzi potrzeba podjęcia działań w celu podniesienia efektywności operacyjnej systemu do założonego poziomu. Tak więc, mierzalne rezultaty działalności pozwalają na ocenę rzeczywistego wykonywania działań istotnych dla bezpieczeństwa w kontekście istniejących w organizacji elementów nadzoru, tak, aby zagrożenia dla bezpieczeństwa mogły być utrzymywane na poziomie najniższym z możliwych przy zachowaniu zdrowego rozsądku (zasada ALARP – **as low as reasonably practicable)** oraz aby mogły zostać podjęte konieczne działania korygujące. Pojęcie to odnosi się zarówno do SSP, jak i SMS, chociaż z pewnymi uwagami, które należy uwzględnić, a które wynikają ze specyfiki każdego z nich, co zostało podkreślone w niniejszej części oraz w podrozdziale 6.6.

6.4.4 Wprowadzenie pojęcia dopuszczalnego poziomu bezpieczeństwa stanowi również odpowiedź na potrzebę połączenia historycznego podejścia do zarządzania bezpieczeństwem opartego na zgodności z przepisami, z podejściem opartym na wynikach. Podejście oparte na wynikach pozwoli ocenić faktyczne wykonywanie działań mających kluczowe znaczenie dla bezpieczeństwa istniejących organizacyjnych systemów kontroli. Cel, jakim jest stałe podnoszenie poziomu bezpieczeństwa, stanowiący podstawę zarządzania bezpieczeństwem, możliwy będzie do osiągnięcia tylko poprzez zapewnienie skutecznego wdrożenia SSP.

6.4.5 Opracowanie i wdrożenie koncepcji akceptowalnego poziomu bezpieczeństwa (ALoS) opiera się na pewnych podstawowych pojęciach z teorii systemów. Zostanie to omówione w dalszej części.

6.4.6 Istnieje pewna hierarchia związana z podstawowymi pojęciami z teorii systemów leżącej u podstaw koncepcji akceptowalnego poziomu bezpieczeństwa i sposób, w jaki pojęcia te należy uporządkować przy opracowywaniu ALoS. Zrozumienie pojęć i związanej z nimi hierarchii jest podstawą dla rozwoju ALoS w odniesieniu do SSP. Stosowane pojęcia i ich hierarchia przedstawiają się następująco:

a) ***bezpieczeństwo*** (zgodnie z definicją opisaną w Rozdziale 2);

b) ***poziom bezpieczeństwa*** – stopień bezpieczeństwa systemu. Jest to zasadnicza cecha systemu, reprezentująca jakość systemu, jego sprzyjanie bezpieczeństwu. Wyrażany jest on poprzez wskaźniki bezpieczeństwa;

c) ***wskaźniki bezpieczeństwa*** – są to parametry charakteryzujące i/lub stanowiące poziom bezpieczeństwa systemu;

d) ***cele bezpieczeństwa*** – są to określone docelowe wartości poziomu bezpieczeństwa, jaki ma być osiągnięty;

e) ***dopuszczalny poziom bezpieczeństwa*** – minimalny stopień bezpieczeństwa, jaki musi zostać zapewniony w praktyce bieżącej działalności;

f) ***wartość wskaźnika bezpieczeństwa*** – kwantyfikacja wskaźnika bezpieczeństwa;

g) ***wartość celu bezpieczeństwa*** – kwantyfikacja celu bezpieczeństwa.

6.4.7 Wybór odpowiednich wskaźników bezpieczeństwa jest kluczowy dla rozwoju koncepcji dopuszczalnego poziomu bezpieczeństwa. Taki wybór powinien być funkcją elementu, dla którego poziom bezpieczeństwa systemu ma być reprezentowany. Jeżeli poziom bezpieczeństwa ma być przedstawiany szeroko, w kategoriach ogólnych, dobór wskaźników bezpieczeństwa reprezentujących wyniki systemu o charakterze mającym duże znaczenie i konsekwencje (wskaźniki ilościowe) oraz wysoki poziom funkcjonowania systemu (wskaźniki jakościowe) jest właściwy. Jeżeli poziom bezpieczeństwa systemu jest przedstawiany w szczegółowych, wąskich kategoriach, wówczas wymagany jest wybór wskaźników reprezentujących wyniki systemu o charakterze mającym małe znaczenie/znikome konsekwencje i niższy poziom funkcjonowania systemu. W obu przypadkach konkretne wskaźniki bezpieczeństwa muszą być reprezentatywne dla wyników, procesów i funkcji, które charakteryzują bezpieczeństwo systemu.

6.4.8 Typowe przykłady wskaźników bezpieczeństwa w systemie lotnictwa zawierają między innymi:

a) wypadki śmiertelne w lotnictwie;

b) poważne incydenty;

c) incydenty opuszczenia pasa;

d) kolizje na ziemi;

e) rozwój/brak podstawowych przepisów w dziedzinie lotnictwa;

f) rozwój/brak przepisów operacyjnych (wykonawczych);

g) poziom przestrzegania przepisów.

6.4.9 Typowe przykłady mierników bezpieczeństwa w systemie lotnictwa zawierają między innymi:

a) zmniejszenie ilości wypadków śmiertelnych w lotnictwie;

b) zmniejszenie ilości poważnych wypadków;

c) zmniejszenie ilości incydentów opuszczenia pasa;

d) zmniejszenie ilości kolizji na ziemi;

e) liczba inspekcji w kwartale.

6.4.10 Pierwszym krokiem w określeniu dopuszczalnego poziomu bezpieczeństwa związanego z SSP jest zatem szczegółowe określenie, jaki poziom bezpieczeństwa danego systemu bezpieczeństwa lotnictwa w państwie ma być ustalany, a następnie wybór konkretnych wskaźników bezpieczeństwa, które będą charakteryzować poziom bezpieczeństwa krajowego systemu lotnictwa. Dostępność do danych odnośnie bezpieczeństwa jest dla państwa czynnikiem decydującym w podejmowaniu decyzji dotyczących szczegółów reprezentacji, jak również doboru ilościowych lub jakościowych wskaźników bezpieczeństwa. Te państwa, które opracowały systemy bezpieczeństwa umożliwiające zbieranie danych i możliwości ich analizy powinny być w stanie reprezentować poziom bezpieczeństwa w sposób bardziej szczegółowy niż państwa, które tego nie zrobiły. Państwa z tej

pierwszej grupy powinny mieć możliwość określenia ilościowych wskaźników bezpieczeństwa, podczas gdy te z grupy drugiej mogą zdecydować się początkowo na jakościowe wskaźniki bezpieczeństwa, dopóki nie rozwiną systemów bezpieczeństwa zbierania danych i możliwości ich analizy. Gdy zostaną już określone wskaźniki bezpieczeństwa, następnym krokiem jest określenie celów związanych z bezpieczeństwem, które to cele mogą być uznane za wskaźniki do poprawienia.

6.4.11 Gdy wskaźniki oraz cele bezpieczeństwa zostaną już wybrane, może zostać ustalony szczegółowy poziom bezpieczeństwa państwowego systemu lotnictwa. W tym momencie, państwo powinno być gotowe do przejścia do etapu określania dopuszczalnego poziomu bezpieczeństwa, czyli minimalnego stopnia bezpieczeństwa w lotnictwie cywilnym, który powinien być zapewniony poprzez SSP w praktyce. W celu określenia dopuszczalnego poziomu bezpieczeństwa, do wskaźników bezpieczeństwa należy dołączyć wartości, a plan poprawy i/lub utrzymania tych wartości powinien być powiązany z celami bezpieczeństwa. Chociaż powszechnie wiadomo, że dopuszczalny poziom bezpieczeństwa w odniesieniu do SSP wyraża się poprzez wartości wskaźników bezpieczeństwa i wartości celów bezpieczeństwa, ściśle rzecz biorąc, to wartości celów bezpieczeństwa są prawdziwym wyznacznikiem dopuszczalnego poziomu bezpieczeństwa. Rysunek 6-1 zawiera przykład wartości wskaźników bezpieczeństwa i wartości celów bezpieczeństwa, które mają zostać osiągnięte. Dalsza uwaga przy ustalaniu dopuszczalnego poziomu bezpieczeństwa powinna być skupiona na następujących elementach:

a) poziomie ryzyka (bezpieczeństwa) jaki ma zastosowanie;

b) tolerancji ryzyka bezpieczeństwa;

c) kosztach/zyskach wprowadzania zmian do systemu lotnictwa;

d) oczekiwaniach społecznych co do systemu lotnictwa cywilnego.

| **Wartość wskaźnika bezpieczeństwa** | | **Wartość celu bezpieczeństwa, jaki ma zostać osiągnięty** |
|---|---|---|
| 1. (*Poziom/liczba*) poważnych wypadków na (liczba) operacji | **=>** | 1. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) poważnych wypadków lotniczych na (*liczba*) operacji |
| 2. (*Poziom/liczba*) *wtargnięć na drogi startowe na (liczba) operacji* | **=>** | 2. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) *wtargnięć na drogi startowe na (liczba) operacji* |
| 3. (*Poziom/liczba*) kolizji na płycie na (liczba) operacji | **=>** | 3. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) kolizji na płycie na (*liczba*) operacji |
| 4. *(Liczba)* zakończonych inspekcji operatorów w (*podanie okresu*) | **=>** | 4. Minimum (*liczba*) zakończonych inspekcji w (*podanie okresu*) |

**Rysunek 6-1. Przykład wartości wskaźników bezpieczeństwa i wartości celów bezpieczeństwa, które mają zostać osiągnięte**

6.4.12 W celu prawidłowego określenia dopuszczalnego poziomu bezpieczeństwa w odniesieniu do SSP, istotne jest również, aby zrozumieć różnicę między dwoma ściśle związanymi ze sobą – a więc niekiedy mylonymi – całkiem odmiennymi pojęciami: pomiarem bezpieczeństwa i pomiarem wyników bezpieczeństwa.

6.4.13 **Analiza** (**pomiar) bezpieczeństwa** odnosi się do kwantyfikacji wybranych wyników poważnych zdarzeń powodujących istotne konsekwencje takich, jak wypadki i poważne incydenty. Pomiar bezpieczeństwa może być również stosowany w celu odzwierciedlenia oznaczania wybranych na wysokim poziomie funkcji państwa, takich jak stan rozwoju /realizacji podstawowych aktów prawnych dotyczących bezpieczeństwa lotnictwa cywilnego lub ich brak, stan rozwoju/ realizacji konkretnych przepisów operacyjnych lub ich braku a poziom przestrzegania przepisów w państwie. Pomiar bezpieczeństwa nie jest ciągłym procesem, ale jest raczej sprawdzany punktowo, zazwyczaj przeprowadzany w z góry określonych ramach czasowych, na przykład, co roku, pół roku lub co kwartał. Pomiar bezpieczeństwa wiąże się z SSP i odzwierciedla, w jakim stopniu założone cele bezpieczeństwa zostały osiągnięte dzięki strategii interwencji i łagodzenia skutków, jako części SSP.

6.4.14 **Analiza** (**pomiar) wyników bezpieczeństwa** odnosi się do kwantyfikacji wybranych wyników poziomu niskiego stopnia, takich jak liczba zdarzeń dotyczących pozostawionych zewnętrznych obiektów-szczątków (foreign object derbis - FOD) na określoną liczbę operacji na ziemi lub liczby nieautoryzowanych incydentów z pojazdem naziemnym na drogach kołowania na konkretną liczbę operacji w portach lotniczych lub w określonym przedziale czasu. Pomiar wydajności bezpieczeństwa dokonywany jest non-stop, obejmuje stałe nadzorowanie i pomiary wybranych działań operacyjnych, które są niezbędne do świadczenia przez organizację usług, dla których organizacja została utworzona (usługi lotniskowe, kontrola ruchu lotniczego, szkolenia itp.). Pomiar wydajności bezpieczeństwa jest najczęściej, ale nie wyłącznie, związany z systemem zarządzania bezpieczeństwem i stanowi miarę rzeczywistych wyników operacyjnych systemów zarządzania, takich jak SSP lub SMS, poza miarą absolutną wynikającą z pomiaru bezpieczeństwa (w tym zgodność z przepisami). Ma również zastosowanie do interwencji w zakresie bezpieczeństwa i strategii ograniczania strat ustanowionych w ramach SSP jako właściwe działania.

6.4.15 Akceptowalny poziom bezpieczeństwa związany z SSP musi być opracowany w oparciu o rozsądne połączenie pomiaru bezpieczeństwa i pomiar wyników w zakresie bezpieczeństwa. W jakim zakresie akceptowalny poziom bezpieczeństwa stanowi miarę bezpieczeństwa lub pomiar poziomu bezpieczeństwa, zależy od dojrzałości SSP. Początkowo, natychmiast po opracowywaniu i wdrażaniu SSP, wartości wskaźników bezpieczeństwa i wartości docelowych bezpieczeństwa związanych z akceptowalnym poziomem bezpieczeństwa prawdopodobnie zostaną wyrażone poprzez ilościowe oświadczenia działań dla wybranych wyników high-level/high-consequence (pomiar w zakresie bezpieczeństwa). Rysunek 6-2 stanowi przykład wartości wskaźników bezpieczeństwa i wartości docelowych bezpieczeństwa opartych na pomiarach bezpieczeństwa.

6.4.16 W miarę jak SSP dojrzewa i bezpieczeństwo gromadzenia i analizy danych wdrażane są przez komponent zapewnienia bezpieczeństwa SSP, wartości wskaźników bezpieczeństwa oraz wartości celów bezpieczeństwa związane z akceptowalnym poziomem bezpieczeństwa mogą zostać zmodyfikowane i wyrażone poprzez połączenie kwantyfikowalnych wyników działania dotyczących wydarzeń o konsekwencjach wysokiego stopnia (pomiar bezpieczeństwa) oraz kwantyfikowalnych wyników działania dotyczących wydarzeń o konsekwencjach niskiego stopnia (pomiar wyników bezpieczeństwa). W momencie, gdy SSP osiągnie dojrzałość, wartości wskaźników bezpieczeństwa i wartości celów bezpieczeństwa związane z akceptowalnym poziomem bezpieczeństwa, będzie wyrażana poprzez ilościowe wyniki działań na wybranych wynikach działania dotyczących wydarzeń o konsekwencjach niskiego stopnia (pomiar wyników bezpieczeństwa). Rysunek 6-3 stanowi przykład wartości wskaźników bezpieczeństwa i wartości celów bezpieczeństwa w oparciu o pomiar poziomu bezpieczeństwa.

6.4.17 Dokonując oceny należy wziąć pod uwagę dwa ogólne aspekty, tj., czy określone wartości docelowe akceptowalnego poziomu bezpieczeństwa powinny reprezentować poprawę czy raczej utrzymanie na bieżącym poziomie związanych z nimi wartości wskaźników bezpieczeństwa. Po pierwsze, należy zastanowić się co do dostępności środków w ramach których państwo może osiągnąć poprawę. Po drugie, należy zastanowić się, za jak kosztowne uznaje się plan(y) działań niezbędnych do osiągnięcia poprawy. Po trzecie rozważyć, jedynie dla wartości docelowych bezpieczeństwa w oparciu o pomiar poziomu bezpieczeństwa, czy oceny ryzyka bezpieczeństwa jako skutków zagrożeń określane poprzez wzrost wchodzą w region dopuszczalnego ryzyka bezpieczeństwa procesu zarządzania, jak omówiono w rozdziale 5. Wartości docelowe bezpieczeństwa mogą w pewnym momencie odzwierciedlać ocenę ryzyka bezpieczeństwa, która mieści się w granicach tolerancji w przeważających przypadkach. Jednakże zmiany w systemie, wzrost itp. może spowodować, że takie oceny ryzyka bezpieczeństwa będą nieważne. Wartości docelowe bezpieczeństwa muszą w tym przypadku odzwierciedlać poprawę w odniesieniu do związanych z nimi wartości wskaźnika bezpieczeństwa ważnego w zmienionym środowisku.

| Wartość wskaźnika bezpieczeństwa | Wartość celu bezpieczeństwa, jaki ma zostać osiągnięty |
|---|---|
| 1. (*Liczba*) CFIT wypadków na podejściu i w fazie lądowania na (l*iczba*) odlotów | 1. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) CFIT wypadków w fazie podejścia i lądowania na (*liczba*) operacji |
| 2. (*liczba*) wtargnięć na drogi startowe na (*liczba*) operacji | 2. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) wtargnięć na drogi startowe na (*liczba*) operacji |
| 3. (*liczba*) kolizji na płycie rocznie na średnio x kolejnych lat | 3. Zmniejszenie o (*liczba*) liczby / maksimum kolizji na płycie na średnio x lat |
| 4. (*liczba*) poważnych zdarzeń wykrytych w ramach krajowego obowiązkowego systemu zgłaszania zdarzeń rocznie | 4. Minimum (*liczba*) poważnych zdarzeń wykrytych w ramach krajowego obowiązkowego systemu zgłaszania zdarzeń rocznie |
| 5. *(liczba*) zakończonych inspekcji operatorów kwartalnie | 5. Minimum (*liczba*) zakończonych inspekcji operatorów kwartalnie |
| 6. (*liczba*) Służb Informacji Lotniczej z wdrożonym systemem zarządzania jakością | 6. (*liczba*) Służb Informacji Lotniczej z wdrożonym systemem zarządzania jakością do (*data*) |
| 7. Elektroniczne nanoszenie różnic zakończone w ciągu (*liczba*) miesięcy/tygodni | 7. Elektroniczne nanoszenie różnic zakończone w ciągu (*uaktualniona liczba*) miesięcy/tygodni |

**Rysunek 6-2. Przykład wartości wskaźnika bezpieczeństwa i wartości celu bezpieczeństwa w oparciu o ocenę bezpieczeństwa**

| Wartość wskaźnika bezpieczeństwa | Wartość celu bezpieczeństwa, jaki ma zostać osiągnięty |
|---|---|
| 1. (*Liczba*) zmian ustalonej wysokości lotu na (*liczba*) operacji | 1. Zmniejszenie o (*liczba*) liczby / maksimum zmian wysokości lotu na (*liczba*) operacji do (*termin*) |
| 2. (*liczba*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (państwowych) na (liczba) operacji | 2. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (państwowych) na (*liczba*) operacji |
| 3. (*Liczba*) zdarzeń związanych z zadziałaniem systemu TCAS/airprox na (*liczba*) operacji | 3. Zmniejszenie o (*liczba*) liczby / maksimum zdarzeń związanych z zadziałaniem systemu TCAS/airprox na (*liczba*) operacji do (*termin*) |
| 4. (*Liczba*) podejść do lądowania niezgodnie z procedurą (NCA) na pięciu lotniskach międzynarodowych (państwowych) na (*liczba*) operacji | 4. Zmniejszenie o (*liczba*) liczby / maksimum podejść do lądowania niezgodnie z procedurą (NCA) na pięciu lotniskach międzynarodowych (państwowych) na (*liczba*) operacji do (*termin*) |
| *5.* (*Liczba*) zdarzeń na płycie związanych z uszkodzeniem statków powietrznych przez ciała obce na pięciu lotniskach międzynarodowych (państwowych) na (*liczba*) operacji | 5. Zmniejszenie o (*liczba*) liczby / maksimum (*liczba*) zdarzeń na płycie związanych z uszkodzeniem statków powietrznych przez ciała obce na pięciu lotniskach międzynarodowych (państwowych) na (*liczba*) operacji do (*termin*) |

**Rysunek 6-3. Przykład wartości wskaźnika bezpieczeństwa oraz wartości celu bezpieczeństwa w oparciu o ocenę wyników i działań w zakresie bezpieczeństwa**

6.4.19 Akceptowalny poziom bezpieczeństwa wdraża się poprzez plany działań. Są to narzędzia i środki niezbędne do osiągnięcia wartości docelowych akceptowalnego poziomu bezpieczeństwa związane z SSP. Plany działania obejmują procedury operacyjne, technologie, systemy i programy, których niezawodność, dostępność, wydajności i/lub dokładności można dokładnie zmierzyć. Przykładem planu działania na rzecz bezpieczeństwa związanego z celem, jakim jest redukcja przypadków CFIT, byłoby wdrożenie stałych procedur przylotów i wykresy procedur przylotów zaprojektowane w celu stabilizacji podejścia. Przykładem planu działania na rzecz bezpieczeństwa związanym z celem, jakim jest ograniczenie zdarzeń wtargnięcia na pas startowy, byłoby wdrożenie systemu radarowego z oczekiwanymi 98 procentami dostępności sprzętu krytycznego.

6.4.20 Należy zdecydowanie powiedzieć, że pojęcie akceptowalnego poziomu bezpieczeństwa odnosi się do celów na poziomie krajowym, które mają być osiągnięte poprzez SSP jako sposób na sprawdzenie zadowalającego wdrożenia SSP. Dlatego zawsze należy stosować odniesienia do akceptowalnego poziomu bezpieczeństwa związanego z SSP. Wartości wskaźników bezpieczeństwa i wartości docelowe akceptowalnego poziomu bezpieczeństwa dostarczają wymiernego sposobu zapewnienia i wykazania skuteczności SSP, poza zgodnością z przepisami. SSP powinien spełniać wszystkie wymogi prawne, jakie zostały określone w przepisach krajowych i międzynarodowych. Zgodność z przepisami leży nadal u podstaw zarządzania bezpieczeństwem. Wybierając połączenie wymiernych wyników operacyjnych działania, które mają charakter państwowy i które zbudowane są na fundamencie zgodności z przepisami, można być pewnym osiągnięcia rzeczywistej skuteczności i efektywności zarządzania bezpieczeństwem procesów leżących u podstaw SSP.

6.4.21 Realizacja akceptowalnego poziomu bezpieczeństwa wykracza poza zgodność z regulacjami krajowymi i międzynarodowymi. Ustanowienie akceptowalnego poziomu bezpieczeństwa dla SSP nie zastępuje regulacji prawnych i innych ustalonych wymagań, ani nie zwalnia państwa z zobowiązań dotyczących Konwencji o międzynarodowym lotnictwie cywilnym (ICAO Doc 7300) i postanowień zawartych w załącznikach do Konwencji.

6.4.22 Podsumowując, rys. 6-4, 6-5 i 6-6 przedstawiają w formie graficznej przejście od początków do dojrzałego akceptowalnego poziomu bezpieczeństwa związanego z SSP, akceptowalny poziom bezpieczeństwa odzwierciedlający pomiar bezpieczeństwa oraz akceptowalny poziom bezpieczeństwa odzwierciedlający pomiar poziomu bezpieczeństwa związany z systemem zarządzania bezpieczeństwem, jak to opisano w tej części rozdziału.

## 6.5 SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM (SMS)

6.5.1 W Załącznikach 1, 6, 8, 11, 13 i 14 ustalono, że państwa wymagają w ramach SSP, by dostawcy usług u których występują zagrożenia bezpieczeństwa w trakcie ich świadczenia, takie jak zatwierdzone organizacje szkoleniowe, operatorzy statków powietrznych, zatwierdzone organizacje obsługi technicznej, organizacje odpowiedzialne za projekty typu i/lub produkcję statków powietrznych, służby ruchu lotniczego i certyfikowane lotniska wdrożyły system zarządzania bezpieczeństwem (SMS). SMS jest narzędziem zarządczym w zakresie zarządzania bezpieczeństwem w organizacji. W załącznikach do Konwencji Chicagowskiej przyjęto także założenie, że SMS będzie uznawany przez państwo i powinien zawierać co najmniej:

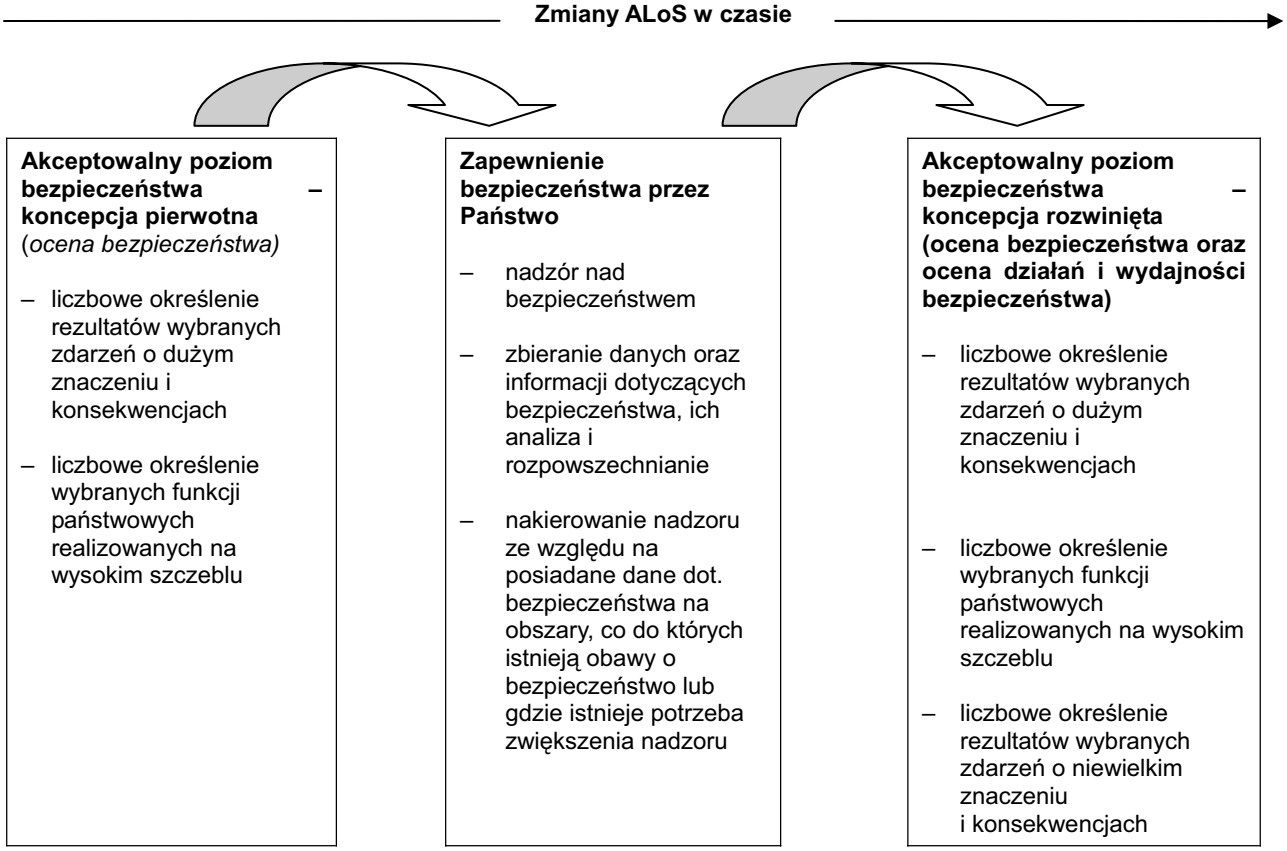
a) identyfikację zagrożeń bezpieczeństwa;

b) zapewnienie wdrożenia niezbędnych działań naprawczych w celu utrzymania założonej wydajności systemu bezpieczeństwa;

c) założenie stałego monitorowania i regularnej oceny wydajności systemu bezpieczeństwa;

d) dążenie do ciągłej poprawy ogólnej wydajności systemu zarządzania bezpieczeństwem.

6.5.2 Cztery powyższe ogólne procesy objęte wymogiem Systemu Zarządzania Bezpieczeństwem ICAO (identyfikacja zagrożeń, wdrożenie działań naprawczych w odpowiedzi na zagrożenie bezpieczeństwa, monitorowanie oraz ciągłe doskonalenie) obejmują cztery podstawowe działania mające na celu rozwiązywanie problemów w zakresie bezpieczeństwa, wspierające świadczenie usług przez organizacje:




**Rysunek 6-4. Przejście od pierwotnej do rozwiniętej koncepcji akceptowalnego poziomu bezpieczeństwa w relacji do Krajowego Programu Bezpieczeństwa (SSP)**

a) ustalenie gdzie tkwi błąd (identyfikacja zagrożenia);

b) zaproponowanie i wdrożenie poprawki lub poprawek (działania naprawcze);

c) upewnienie się, że proponowana poprawka lub poprawki są zgodne z przeznaczeniem (stały monitoring);

d) nieustanne udoskonalanie systemu zarządzania w celu zapewnienia skuteczności i efektywności świadczenia usług (ciągłe doskonalenie systemu zarządzania bezpieczeństwem).

6.5.3 SMS jest definiowany jako systematyczne podejście do zarządzania bezpieczeństwem, obejmujące niezbędne struktury organizacyjne, zakres odpowiedzialności, zasady i procedury. Podstawy systemu zarządzania bezpieczeństwem zostały omówione w rozdziale 7. Podobnie jak w przypadku SSP, Organizacja Międzynarodowego Lotnictwa Cywilnego opracowała pewną ogólną strukturę systemu zarządzania bezpieczeństwem, aby pomóc dostawcom usług świadczącym usługi lotnicze w opracowaniu i wdrożeniu systemu zarządzania bezpieczeństwem. Wspomniana struktura składa się z czterech komponentów i dwunastu elementów, które zostały przedstawione szczegółowo w rozdziałach 8 i 9.

### 6.6 SMS A POZIOM REALIZACJI BEZPIECZEŃSTWA

6.6.1 W Załącznikach ICAO 1, 6, 8, 11, 13 i 14 ustalono, że SMS dostawcy usług powinien zapewniać działania naprawcze w celu utrzymania poziomu bezpieczeństwa, stale monitorować i regularnie dokonywać oceny tych wyników w zakresie bezpieczeństwa.

6.6.2 Pojęcie realizacji lub inaczej efektywności czy wydajności bezpieczeństwa jest podstawowym elementem skutecznego działania systemu zarządzania bezpieczeństwem, tak samo, jak dążenie w kierunku środowiska regulacyjnego opartego na realizacji i efektywności. Koncepcja poziomu realizacji bezpieczeństwa pomaga w procesie monitorowania bieżącej efektywności systemu zarządzania bezpieczeństwem i pozwala

uniknąć mechanicznego działania typu "zaznacz odpowiednie pole". Dla celów systemu zarządzania bezpieczeństwem konieczne jest określenie zestawu mierzalnych wyników działania w celu ustalenia, czy system rzeczywiście działa zgodnie z założeniami – nie tylko poprzez proste spełnianie wymogów prawnych – oraz do określenia, gdzie może być konieczne podjęcie działań w celu dostosowania wydajności systemu zarządzania bezpieczeństwem do oczekiwanego poziomu. Owe mierzalne wyniki pozwalają na ocenę rzeczywistej efektywności działań, krytycznych dla bezpieczeństwa w kontekście istniejących organizacji kontroli, tak, aby możliwe było podejmowanie niezbędnych działań naprawczych oraz utrzymanie zagrożeń dla bezpieczeństwa na poziomie najniższym z możliwych (ALARP).

6.6.3 Podejście oparte na wynikach będzie oceniać rzeczywistą efektywność działań krytycznych dla bezpieczeństwa w kontekście istniejących organizacji kontroli. Ponadto, tylko przez zapewnienie skutecznego działania i realizowania bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem – poprzez ustanowienie i pomiar konkretnych wyników wykonania bezpieczeństwa – możliwe jest osiągnięcie celu, jakim jest ciągła poprawa skutecznego zarządzania bezpieczeństwem.

6.6.4 Wyniki bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem nie są powiązane z liczbowym określeniem rezultatów, charakteryzujących się poważnymi konsekwencjami (ocena bezpieczeństwa), ale raczej z liczbowym określeniem procesów mających znikome znaczenie i konsekwencje (pomiar poziomu realizacji/efektywności bezpieczeństwa). Poziom wykonania bezpieczeństwa przez SMS reprezentuje wyłącznie pomiar skuteczności działań podejmowanych w obszarze i na rzecz bezpieczeństwa. Poziom realizacji bezpieczeństwa wyraża cele bezpieczeństwa dostawcy usług w postaci mierzalnych wyników bezpieczeństwa w konkretnych procesach realizowanych na niższych szczeblach w systemie zarządzania bezpieczeństwem. Z perspektywy relacji pomiędzy państwem a dostawcami usług, podejmowane działania i ich efekty w zakresie bezpieczeństwa umożliwiają państwu w obiektywny i przejrzysty sposób dokonanie pomiaru efektywności lub inaczej skuteczności, jaką powinien osiągnąć posiadany przez dostawców SMS, podczas realizacji ich podstawowych zadań. Taka wydajność i wykonanie działań w obszarze bezpieczeństwa powinny być uzgodnione pomiędzy Państwem i dostawcami usług, jako dopuszczalne minimum, które dostawcy usług muszą osiągnąć w procesie świadczenia usług. Poziom wykonania bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem jest więc odniesieniem, w stosunku do którego państwo może dokonywać oceny poziomu bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem, co dalej oznacza, że SMS wykracza ponad działania wyłącznie zgodne z procedurami. Przy uzgadnianiu poziomu wykonania bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem, należy rozważyć takie czynniki, jak stopień zagrożenia bezpieczeństwa, koszty/korzyści wynikające z poprawy systemu oraz oczekiwania społeczne co do bezpieczeństwa w branży lotniczej.

6.6.5 W obrębie każdego państwa, efektywność i poziom wykonania bezpieczeństwa każdego systemu zarządzania bezpieczeństwem zostaną uzgodnione odrębnie pomiędzy państwem, a poszczególnymi organizacjami lotnictwa. Uzgodnione zakładane wykonanie i efektywność bezpieczeństwa powinny być współmierne do stopnia skomplikowania poszczególnych organizacji lotniczych, działających w specyficznych uwarunkowaniach operacyjnych oraz odnosić się równocześnie do możliwości i dostępności posiadanych przez organizacje lotnicze zasobów. W praktyce poziom realizacji bezpieczeństwa przez SMS jest wyrażany poprzez wartość wskaźnika poziomu realizacji bezpieczeństwa i docelową wartość wskaźnika poziomu realizacji bezpieczeństwa i jest wdrażany poprzez plany działania.

6.6.6 Wartości wskaźnika poziomu realizacji bezpieczeństwa są krótkoterminowymi, mierzalnymi celami odzwierciedlającymi wykonanie i efektywność bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem. Są one wyrażane w kategoriach liczbowych; powinny być jasne, wymierne i powiązane z zagadnieniami bezpieczeństwa objętymi działaniem systemu zarządzania bezpieczeństwem. Wartości wskaźnika poziomu realizacji bezpieczeństwa odzwierciedlają wyłącznie pomiar wykonania bezpieczeństwa. Wartości wskaźnika poziomu realizacji bezpieczeństwa systemu zarządzania bezpieczeństwem nie powinny odzwierciedlać oceny bezpieczeństwa. Ponieważ wykonanie i poziom efektywności bezpieczeństwa każdego systemu zarządzania bezpieczeństwem zostaną uzgodnione odrębnie pomiędzy państwem a poszczególnymi organizacjami lotniczymi, wartości wskaźnika poziomu realizacji bezpieczeństwa będą się różnić między segmentami i poszczególnymi dostawcami usług działającymi w sektorze lotniczym, takimi jak operatorzy statków powietrznych, certyfikowani operatorzy lotniskowi i dostawcy usług w zakresie ruchu lotniczego. Przykład poniżej.

6.6.7 Poprzez swój SMS, certyfikowany operator lotniskowy zidentyfikował pewne istotne z punktu widzenia bezpieczeństwa zdarzenia w postaci szczątków ciał obcych (FOD) znajdujących się na płycie lotniska, pozostałych podczas wykonywania operacji na płycie. Zidentyfikował również niepokojące zdarzenia dotyczące ruchu nieupoważnionych pojazdów po drogach kołowania. Dlatego też operator określa następujące wartości wskaźnika poziomu realizacji bezpieczeństwa, w porozumieniu z państwowym organem nadzoru lotniczego: 15 zdarzeń związanych z pojawieniem się szczątków ciał obcych na płycie lotniska na 10 000 operacji i 20 zdarzeń związanych z nieuprawnionym wtargnięciem pojazdów na drogi kołowania na 10 000 operacji. Te wartości wskaźnika wykonania i wydajności bezpieczeństwa spełniają warunki omówione w pkt. 6.6.6: tzn. są oczywiste i jasne, wyrażone w postaci liczbowej, można je zmierzyć i powiązać z zagadnieniami bezpieczeństwa zawartymi w lotniskowym systemie zarządzania bezpieczeństwem lotniska. Ponadto obydwa wskaźniki wykonania bezpieczeństwa odzwierciedlają pomiar i ocenę wydajności bezpieczeństwa.

6.6.8 Docelowe wartości poziomu wykonania bezpieczeństwa mają charakter długoterminowych, mierzalnych celów odzwierciedlających wydajność lub inaczej wykonanie bezpieczeństwa przez SMS. Docelowe wartości poziomu realizacji bezpieczeństwa wyrażane są w kategoriach liczbowych, powinny one być oczywiste i wymierne, akceptowalne i możliwe do przyjęcia przez zainteresowanych, i związane ze wskaźnikiem poziomu realizacji bezpieczeństwa (krótkoterminowym celem) przez SMS.

| | |
|---|---|
| **Ilościowe określenie celów bezpieczeństwa do osiągnięcia** | 1. Zredukować o (*wskazanie liczby)* liczbę / maksymalnie (*wskazanie liczby*) podejść CFIT oraz wypadków przy lądowaniu w stosunku do (*wskazanie liczby*) odlotów.<br>2. Minimum (podanie liczby) inspekcji operatorów przeprowadzonych w okresie kwartału.<br>3. **…..** |
| **Plan działań w stosunku do określonych celów** | 1. Cykl szkoleń w zakresie CFIT rozpropagowany wśród dostawców usług działających na rynku i poparty kursami szkoleniowymi.<br>2. Przegląd i jeśli to konieczne uaktualnienie polityki w zakresie zatrudniania. Uaktualnienie podręcznika inspekcjonowania.<br>3. … |
| **Wartości wskaźnika bezpieczeństwa** | 1. (*Wskazanie liczby)* wypadków związanych z CFIT oraz podczas wykonywania procedury podejścia i lądowania w stosunku do (*wskazanie liczby*) odlotów.<br>2. (*Wskazanie liczby*) inspekcji operatorów przeprowadzonych w okresie kwartału.<br>3. … |

**Tabela 6-5. Akceptowalny poziom bezpieczeństwa jako odzwierciedlenie oceny bezpieczeństwa**

| | |
|---|---|
| **Ilościowe określenie celów bezpieczeństwa do osiągnięcia** | 1. Zredukować o (*wskazanie liczby)* liczbę / maksymalnie (*wskazanie liczby*) niezgodnych podejść (NCA) na pięciu lotniskach międzynarodowych w stosunku do (*wskazanie liczby*) przylotów w terminie do (*podanie daty*).<br>2. Zmniejszyć o (*wskazanie liczby*) liczbę / maksymalnie (*wskazanie liczby*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (*nazwa kraju*) w stosunku do (*wskazanie liczby*) operacji w terminie do (*podanie daty*).<br>3. **…..** |
| **Plan działań w stosunku do określonych celów** | 1. Wdrożenie procedur ciągłego zniżania (constant descent arrival – CDA). Opracowanie projektów graficznych procedur podejścia dla ustabilizowanego, ciągłego zbliżania.<br>2. Instalacja ASDE/X na pięciu międzynarodowych lotniskach (*nazwa kraju*).<br>3. … |
| **Wartości wskaźnika bezpieczeństwa** | 1. (*Wskazanie liczby)* niezgodnych podejść (non-conforming approaches-NCA) na pięciu lotniskach międzynarodowych w stosunku do (*wskazanie liczby*) operacji.<br>2. (*Wskazanie liczby*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (*nazwa kraju*) w stosunku do (*wskazanie liczby*) operacji.<br>3. … |

**Tabela 6-6. Akceptowalny poziom bezpieczeństwa jako odzwierciedlenie oceny wydajności i stopnia realizacji bezpieczeństwa**

6.6.9 Kontynuując przykład omówiony w pkt. 6.6.7., lotnisko określa następujące wartości docelowe poziomu realizacji bezpieczeństwa, w porozumieniu z państwowym organem nadzoru lotnictwa cywilnego: w styczniu 2009 r., ograniczenie zdarzeń typu FOD (ciała obce na płycie lotniska) do 8 na 10 000 operacji i utrzymanie 20 zdarzeń związanych z nieuprawionym wtargnięciem pojazdów na drogi kołowania na 10 000 operacji. Te wartości docelowe wykonania bezpieczeństwa spełniają warunki omówione w pkt. 6.6.6: są wyrażone w kategoriach liczbowych, są jasne, wymierne i powiązane ze wskaźnikami wydajności bezpieczeństwa lotniskowego systemu zarządzania bezpieczeństwem. Ponadto obydwie wartości docelowe poziomu realizacji bezpieczeństwa odzwierciedlają pomiar i ocenę efektywności bezpieczeństwa.

6.6.10 Plany działania to narzędzia i środki niezbędne do osiągnięcia wartości wskaźnika wydajności bezpieczeństwa i wartości docelowej wydajności bezpieczeństwa systemu zarządzania bezpieczeństwem. Obejmują one procedury operacyjne, technologie, systemy i programy, dla których można dokładnie określić środki niezawodności, dostępności, wydajności i/lub dokładności. Przykładem planu działań w celu osiągnięcia wartości

wskaźnika poziomu realizacji bezpieczeństwa i wartości docelowej poziomu realizacji bezpieczeństwa systemu zarządzania bezpieczeństwem, o których mowa powyżej, będą: wdrożenie programu inspekcji rampy trzy razy dziennie, opracowanie i wdrożenie szkolenia dla kierowców i zastosowanie specyficznego dla danego lotniska oznakowania dróg kołowania.

6.6.11 Wartości wskaźnika poziomu wykonania bezpieczeństwa i docelowe wartości poziomu wykonania bezpieczeństwa przez SMS mogą być różne lub takie same. Oceniając czy wskaźniki są takie same czy różne należy wziąć pod uwagę trzy aspekty. Po pierwsze, należy zastanowić się nad dostępem dostawcy usług do środków, dzięki którym będzie on w stanie zmienić wartość wskaźnika poziomu realizacji bezpieczeństwa w bardziej wymagającą wartość docelowej wydajności bezpieczeństwa. Po drugie, należy zastanowić się, jak kosztowne są plany działań uznanych za niezbędne, aby zmienić wartości wskaźnika wydajności bezpieczeństwa na bardziej wymagające wartości docelowej wydajności bezpieczeństwa. Po trzecie i najważniejsze, należy rozważyć, czy ocena ryzyka zagrożenia podana przez wskaźnik wydajności bezpieczeństwa i docelową wydajność bezpieczeństwa leży w granicach tolerancji procesu zarządzania bezpieczeństwem omówionego w rozdziale 5, wówczas wartości wskaźnika wydajności bezpieczeństwa i wartości docelowej wydajności bezpieczeństwa systemu zarządzania bezpieczeństwem powinny być takie same. Wartość wskaźnika wydajności bezpieczeństwa może odzwierciedlać wartość wskaźnika oceny ryzyka, która mieści się w granicach tolerancji dla danego obszaru w określonych warunkach. Jednak zmiany w systemie, wzrost itp. mogą spowodować, że takie oceny ryzyka będą nieważne. Wartość wskaźnika poziomu wykonania bezpieczeństwa należy w tym przypadku przekształcić w bardziej wymagającą wartość docelową poziomu realizacji bezpieczeństwa, która zachowa swoją ważność w zmienionym środowisku.

6.6.12 Szereg różnych wskaźników poziomu realizacji bezpieczeństwa i wartości docelowej poziomu wykonania bezpieczeństwa zapewnia dużo lepszy wgląd w wykonanie bezpieczeństwa przez SMS organizacji lotniczej niż stosowanie jednego wskaźnika lub celu. Innymi słowy, poziom realizacji bezpieczeństwa systemu zarządzania bezpieczeństwem zawsze będzie wyrażony przez kilka wskaźników wykonania bezpieczeństwa i wartości docelowej wykonania bezpieczeństwa, a nigdy nie przez jeden. Dodatkowe przykłady są podane poniżej.

6.6.13 Operator statku powietrznego zidentyfikował fazy podejścia i lądowania podczas wykonywania operacji lotniczych, jako jedną z głównych kwestii mających znaczenie dla bezpieczeństwa, i które mają być uwzględnione przez SMS. Sformułował także, poprzez komponent oceny ryzyka SMS, obawy dotyczące bezpieczeństwa niestabilnego (lub nieodpowiedniego) podejścia do tych lotnisk, sieci obsługiwanych przez podejścia nieprecyzyjne. Dlatego też określa następujące wartości wskaźnika wydajności bezpieczeństwa, w wyniku porozumienia z organem państwowego nadzoru lotniczego: 10 niestabilnych (lub nieodpowiednich) podejść do lądowania na 1 000 operacji w portach lotniczych. Następnie operator statku powietrznego określa następujące wyniki w zakresie wartości docelowej wydajności bezpieczeństwa, w wyniku porozumienia z organem państwowego nadzoru lotniczego: w ciągu najbliższych trzech lat zmniejszenie o pięćdziesiąt procent liczby niestabilnych (lub nieodpowiednich) podejść do lądowania na 1 000 operacji w portach lotniczych stosujących podejścia nieprecyzyjne. Plan działania w celu osiągnięcia wartości wskaźnika wydajności bezpieczeństwa i wartości docelowej wydajności bezpieczeństwa omówione powyżej, byłyby następujące: wdrożenie procedury stałego kąta schodzenia (CDA) przy wykonywaniu zbliżania do lotnisk stosujących podejścia nieprecyzyjne.

6.6.14 Dostawca ATS określił operacje lotniskowe, jako główne zagrożenia dla bezpieczeństwa, które mają być uwzględnione w SMS. Sformułował także, poprzez komponent oceny ryzyka SMS, zagrożenia dla bezpieczeństwa wtargnięciem na pas startowy i określił wartość wskaźnika wydajności bezpieczeństwa na: 0,8 kat. A i B (najpoważniejsze) wtargnięcia na pas startowy na milion operacji w 2009 r. Następnie dostawca ATS określa wartość docelową wydajności bezpieczeństwa: do 2010 r. zmniejszyć kat. A i B (najpoważniejszych) wtargnięć na pas startowy do wysokości nie więcej niż 0,5 na milion operacji.

6.6.15 Wydajność bezpieczeństwa SMS należy określić, na ile to możliwe, poprzez ilościowe wartości wskaźnika wydajności bezpieczeństwa i wartość docelową wydajności bezpieczeństwa. Uznaje się jednak, że w wielu państwach gromadzenie i analiza danych dotyczących bezpieczeństwa dostawców usług nie mogą być w pełni rozwinięte. Ponieważ takie możliwości są opracowywane, wydajność bezpieczeństwa SMS może być określona poprzez kombinację ilościowych i jakościowych wartości wskaźnika wydajności bezpieczeństwa i wartości docelowej wydajności bezpieczeństwa. Docelowo jednak wydajność bezpieczeństwa SMS powinna być definiowana wyłącznie przez wartości ilościowe.

6.6.16 Określenie wydajności bezpieczeństwa SMS jest wymogiem wykraczającym poza zgodność z wymaganiami krajowymi i międzynarodowymi. Ustalenie wydajności bezpieczeństwa SMS nie zastępuje regulacji prawnych i innych ustalonych wymagań, ani nie zwalnia dostawców usług z ich zobowiązań wynikających z odpowiednich przepisów krajowych i tych wynikających z Konwencji o międzynarodowym lotnictwie cywilnym (ICAO Doc 7300) oraz przepisów zawartych w załącznikach do Konwencji.

### 6.7 ZARZĄDZANIE ODPOWIEDZIALNOŚCIĄ

6.7.1 Trzecią i ostatnią grupą w normach oraz zalecanych metodach i zasadach postępowania ICAO, znajdujących się w Załącznikach 1, 6, 8, 11, 13 i 14 dotyczących zarządzania bezpieczeństwem jest odpowiedzialność kierownictwa za zarządzanie bezpieczeństwem w trakcie świadczenia usług. Normy oraz zalecane metody i zasady postępowania ICAO mówią, iż przyjęty SMS musi jasno określić zakresy odpowiedzialności u wszystkich zatwierdzonych organizacji szkoleniowych, które są narażone na zagrożenia bezpieczeństwa w trakcie świadczenia usług, operatorów statków powietrznych, zatwierdzonych organizacji obsługi technicznej, organizacje odpowiedzialne za projekt typu i/lub wytwarzanie statków powietrznych, zapewniających obsługę ruchu lotniczego i na certyfikowanych lotniskach, w tym bezpośrednią odpowiedzialność za bezpieczeństwo części kierownictwa wyższego szczebla.

6.7.2 Wkład kierownictwa w zarządzanie bezpieczeństwem jest omówiony w rozdziałach 3 i 8 i brak dalszych dyskusji jest zasadny. Należy jednak wspomnieć o kwestii językowej: stosowanie terminu odpowiedzialności ze względu na wymogi zarządzania bezpieczeństwem ICAO. W języku angielskim pojęcia ***accountability*** nie należy mylić z pojęciem ***responsibility***. *Responsibility* odnosi się do sytuacji, w której osoba musi wykonać konkretne działania, podczas gdy *accountability* rozciąga się do obowiązku lub gotowości do przyjęcia odpowiedzialności za realizację tych działań. Przy użyciu pojęć z zakresu zarządzania bezpieczeństwem, zakresy odpowiedzialności za bezpieczeństwo (*safety responsibilities*) opisuje związany z bezpieczeństwem cel czynności wymaganych od danej osoby. Zakresy odpowiedzialności za bezpieczeństwo (*safety accountability statements*) wskazują, co dana osoba ma osiągnąć, bezpośrednio lub poprzez nadzór lub zarządzanie innymi, włącznie z tymi, którym ta osoba powierzyła część własnych obowiązków. Różnica pomiędzy tymi dwoma terminami jest znacząca, chociaż jest to różnica istniejąca jedynie w języku angielskim. Stąd termin odpowiedzialności w odniesieniu do zarządzających, według wymagań ICAO zarządzania bezpieczeństwem, jako zawarty w innych niż angielskojęzyczne wersjach Załączników 1, 6, 8, 11, 13 i 14 musi być rozumiany w znaczeniu nadanym przez język angielski określeniu **Accountability.**

6.7.3 Skuteczne zarządzanie bezpieczeństwem wymaga aktywnego uczestnictwa wszystkich szczebli zarządzania i nadzoru. Powinno to być odzwierciedlone w strukturze organizacyjnej i w opublikowanej odpowiedzialności w zakresie bezpieczeństwa. Organizacja powinna określić, udokumentować i ogłosić – przy pomocy schematów organizacyjnych i wykresów – obowiązki, odpowiedzialności i organy. Odpowiedzialności kierownictwa wyższego szczebla i obowiązki służbowe są omówione w rozdziale 8.

### 6.8 Relacja pomiędzy SSP a SMS

6.8.1 Pełne zrozumienie relacji między Krajowym Programem Bezpieczeństwa (SSP) i Systemem Zarządzania Bezpieczeństwem (SMS) jest niezbędne do podjęcia wspólnych działań w ramach zarządzania bezpieczeństwem państwa. Relacja ta może być wyrażona w najprostszych warunkach: państwo jest odpowiedzialne za wdrożenie i rozwój SMS; dostawcy usług są odpowiedzialni za wdrożenie i rozwój Systemu Zarządzania Bezpieczeństwem. Jest to bardzo ważny punkt: państwo nie powinno przygotowywać SMS, to raczej SSP spełnia równoważną rolę. Niemniej jednak państwo jest odpowiedzialne, w ramach działalności jego SSP, za nadzorowanie rozwoju, wdrażania i funkcjonowania SMS u dostawcy usług. W nadzorowaniu poziomu bezpieczeństwa SMS dostawcy usług, pojęcie dopuszczalnego poziomu bezpieczeństwa określone w SSP, jak zostało to omówione w punkcie 6.4, odgrywa podstawową rolę w stosunkach między SSP oraz SMS. Powiązanie między SSP i SMS zostało przedstawione na rysunku 6-7 i jest omówione w rozdziale 11.

6.8.2 Rozdział 3 omawia potencjalny dylemat zarządzania, który może wyniknąć z perspektywy dotyczącej tego, że zarządzanie bezpieczeństwem jest procesem organizacyjnym, a bezpieczne zarządzanie podstawową funkcją biznesową. Taki potencjalny dylemat, przedstawiony jako "dylemat dwóch P" zapewnia odpowiednie tło do wyjaśnienia relacji między SSP oraz SMS.

6.8.3 Na rysunku 6-7 SSP znajduje się po chronionej stronie równowagi między protekcją i produkcją. SSP ma na celu zapewnienie bezpieczeństwa publicznego poprzez kontrolę zagrożeń dla bezpieczeństwa na poziomie państwa. SSP nie ma celów produkcyjnych jako takich. Mimo, że oczekuje się wydajności od państwowych organizacji lotniczych, nie mają one konkretnych produktów lub usług mających na celu zwiększenia zysków. Podstawowym celem państwa poprzez SSP, jest zapewnienie, w miarę możliwości, powszechnego bezpieczeństwa w trakcie świadczenia usług przez ich dostawców. Cel ten osiąga się poprzez określenie akceptowalnego poziomu bezpieczeństwa w ramach SSP, a także poprzez ocenę ryzyka dla bezpieczeństwa w kraju przez dwa "elementy operacyjne" z SSP: zarządzanie ryzykiem i zapewnienie bezpieczeństwa.

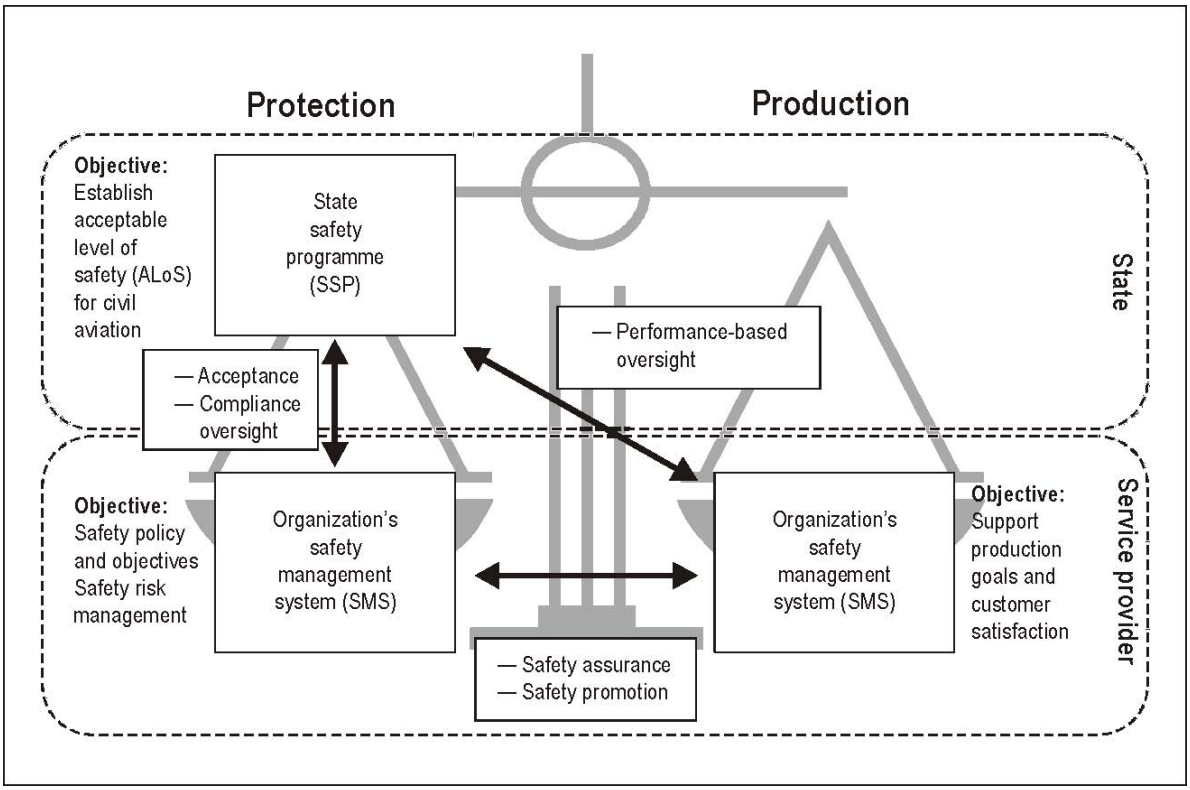



**Figure 6-7. Relationship between an SSP and an SMS**

6.8.4 SMS dostawcy usług tylko częściowo znajduje się po ochronnej stronie równowagi. W odróżnieniu od państwa, dostawca usług ma dostarczyć konkretnych rezultatów w formie produktów i usług, mających przynieść zysk. Celem SMS dostawcy usług w zakresie ochrony jest kontrola zagrożeń będących konsekwencją działań i procesów związanych z dostawą towarów lub usług, w których organizacja się specjalizuje. Dostawca usług osiąga kontrolę nad ryzykiem w trakcie świadczenia usług głównie poprzez dwa "elementy operacyjne" z Systemem Zarządzania Bezpieczeństwem: zarządzanie ryzykiem i zapewnienia bezpieczeństwa, zaś polityka i cele bezpieczeństwa oraz promocja bezpieczeństwa odgrywają pomocniczą lecz ważną rolę.

6.8.5 Państwo, w ramach swoich SSP, początkowo akceptuje SMS dostawcy usług. Akceptacja ta jest głównie nakazowa: państwo, najprawdopodobniej za pośrednictwem organu nadzoru lotnictwa cywilnego, sprawdzi, czy poszczególne części i elementy zaproponowane w Systemie Zarządzania Bezpieczeństwem dostawcy usług są zgodne z obowiązującymi przepisami i wytycznymi ogłoszonymi przez państwo. Ważne jest, aby pamiętać, że akceptacja jest w większości przypadków procesem administracyjnym: państwo zatwierdza projekt systemu zarządzania i planu działań na rzecz jego rozwoju i wdrażania. Krótko mówiąc, akceptacja oznacza głównie "zaznacz odpowiednie pole". Ale przyjęcie, przy jednoczesnym zapewnieniu zgodności z wymogami przepisów, nie gwarantuje właściwego wykonania Systemu Zarządzania Bezpieczeństwem. Przyjmowanie i nadzór nad przestrzeganiem oznaczone są pionowymi strzałkami łączącymi SSP oraz SMS na rys. 6-7. Droga do zapewnienia prawidłowego wykonywania SMS (czy SMS naprawdę działa) musi być nadzorowana przez państwo podczas faktycznego wykonywania działań mających na celu świadczenie usług.

6.8.6 W celu sprawdzenia wydajności Systemu Zarządzania Bezpieczeństwem, państwowy organ nadzoru lotnictwa cywilnego ma za zadanie prowadzić nadzór nad jego skutecznością, okresowo w trakcie świadczenia usług. Może się to okazać trudne lub wręcz niemożliwe do wykonania w praktyce, stąd wskaźniki wydajności bezpieczeństwa i wskaźniki docelowe bezpieczeństwa w SMS. Podczas gdy akceptacja i nadzór nad zgodnością w sposób opisany w punkcie 6.8.5 są oparte na nakazie, o tyle nadzór nad wskaźnikami wydajności bezpieczeństwa i wskaźnikami docelowymi jest uzależniony od wydajności. Pojęcie wydajności bezpieczeństwa omówione w punkcie 6.6 rozciąga się na SMS dostawcy usług, natomiast pojęcie akceptowalnego poziomu bezpieczeństwa określone w ramach SSP omówione w rozdziale 6.4. zatytułowanym: Poziom bezpieczeństwa, jest tym dla SMS, czym akceptowalny poziom bezpieczeństwa jest dla SSP.

6.8.7 Pomiar efektywności bezpieczeństwa SMS zawiera zdefiniowanie wskaźników efektywności bezpieczeństwa, cele wskaźników bezpieczeństwa oraz planów działania. Te kluczowe wskaźniki i cele są reprezentatywne dla ogólnych zagrożeń w kontekście operacyjnym, w którym dostawca usług prowadzi działalność

oraz zapewniają oparty na wynikach procesu nadzoru z uczciwym obrazem wykonania SMS. Poprzez priorytetowe zdefiniowanie zestawu krótko-i średnioterminowych celów, charakterystycznych dla danego dostawcy usług, poprzez wdrażanie strategii łagodzenia skutków ryzyka dla określonych celów bezpieczeństwa, poprzez ustalenie mierników i terminów, umożliwiających pomiar skuteczności strategii łagodzenia skutków, dostawca usług dostarcza organowi nadzoru wymiernych środków w celu sprawdzenia poziomu bezpieczeństwa SMS lub jego braku, poza zgodność z przepisami.

6.8.8 Przerzucenie dyskusji na stronę produkcyjną wagi, zawierającej kompromisy pomiędzy protekcją i produkcją na rys. 6-7 SSP, jak już wspomniano, nie ma celów produkcyjnych jako takich, ale dostawcy usług je mają. Celem działalności dostawcy usług jest osiągnięcie celów handlowych i satysfakcja klienta. SMS stanowi środek z jakiego dostawca usług korzysta w celu zapewnienia, że zagrożenie bezpieczeństwa jako skutek niebezpieczeństw musi być mierzone/pokazywane podczas realizacji celów organizacji produkcji i pozostaje pod kontrolą. SMS dostawcy usług identyfikuje zagrożenia bezpieczeństwa i łagodzenie skutków niezbędne do utrzymania ich w ramach organizacyjnych kontroli poprzez zarządzanie ryzykiem bezpieczeństwa na początku. W momencie, gdy dochodzi do rozpoczęcia działań, kontrola zagrożeń bezpieczeństwa i monitorowania dokonuje się poprzez ciągły proces zapewniania bezpieczeństwa, wspierany przez promowanie bezpieczeństwa. Zarządzanie ryzykiem bezpieczeństwa, zapewnienie bezpieczeństwa i promocja bezpieczeństwa sprawia, że środki dla organizacji w celu utrzymania równowagi pomiędzy produkcją i ochrony są zapewnione.

6.8.9 Ponieważ tradycyjnie rola państwa odnosi się do przyjęcia SMS i nadzoru administracyjnego w zakresie przestrzegania przepisów, jest reprezentowana po stronie ochrony, SSP pełni również rolę w funkcji nadzoru w procesie świadczenia usług. Braki w identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa, jak również w rozwoju strategii łagodzenia skutków, często są związane z alokacją zasobów. Zwykle dzieje się tak w przypadku, gdy podział środków cechuje przychylne nastawienie do działalności produkcyjnej. Braki w identyfikacji zagrożeń i zarządzania ryzykiem, jak również w opracowaniu strategii łagodzenia skutków będą również widoczne przez niezdolność do spełnienia uzgodnionych poziomów bezpieczeństwa SMS dostawcy usług, ze względu na nierówną alokację zasobów do produkcji i ochrony. Dlatego, w wykonywaniu/sprawowaniu nadzoru opartego na wyniku/skuteczności, jaki opisano w punkcie 6.8.7, w nadzorowaniu wydajności operacyjnej SMS w porównaniu z ustaloną wydajnością SMS dla konkretnego dostawcy usług, przychylność w alokacji zasobów, jak również wydajność SMS jako całości, stanie się oczywista: brak środków doprowadzi albo do braku identyfikacji zagrożeń lub nieprawidłowego zarządzania ryzykiem, a tym samym niskiej wydajność SMS. W takim przypadku, choć może zgodny z przepisami, SMS dostawcy usług nie będzie skuteczny. Na rysunku 6-7, oparte na wynikach akceptacja i nadzór są reprezentowane przez strzałki przekątnej łączącej SSP i organizacji procesów produkcyjnych.

### 6.9 ZGODNOŚĆ Z PRZEPISAMI I WYDAJNOŚĆ

6.9.1 Obecnie w lotnictwie daje się zaobserwować rosnące przekonanie o potrzebie uzupełnienia istniejącego podejścia do bezpieczeństwa opartego na zgodności z normami i przepisami (compliance) o podejście związane z realizacją działań i efektach tych działań (performance). Zmiana ta ma na celu rzeczywiste wdrożenie zwyczajów i praktyk zarządzania bezpieczeństwem w ramach SSP oraz SMS. Temat ten został już omówiony w tym rozdziale w części dotyczącej SSP oraz w towarzyszącej części dotyczącej akceptowalnego poziomu bezpieczeństwa. W tej części przedstawione zostało jedynie podsumowanie wcześniejszych rozważań i wniosków, z podkreśleniem najważniejszych kwestii.

6.9.2 Dążenie do zarządzania bezpieczeństwem i podejście do kwestii bezpieczeństwa oparte na realizacji działań i wynikach działań opiera się na wdrożeniu i efektywnym wykorzystywaniu kontroli ryzyka w odniesieniu do bezpieczeństwa. Z punktu widzenia państwa, najbardziej skutecznym sposobem kontroli ryzyka w bezpieczeństwie, pozostającą w jego dyspozycji, są przepisy dotyczące bezpieczeństwa.

6.9.3 W środowisku, w którym bezpieczeństwo realizowane jest poprzez wykazywanie zgodności, podejście do zarządzania bezpieczeństwem jest sztywne i nakazowe, co zostało omówione w rozdziale 3 oraz w niniejszym rozdziale. W środowisku opartym na zgodności, przepisy dotyczące bezpieczeństwa są stosowane jako środki kontroli administracyjnej. Ścisłe ramy regulacyjne są wspierane przez inspekcje i audyty mające jeden wyłączny cel: zapewnienie zgodności z obowiązującymi przepisami.

6.9.4 W środowisku, w którym bezpieczeństwo realizowane jest w oparciu o wyniki działań (performance) – wydajność, podejście charakteryzuje się elastycznością i jest dynamiczne. W takim środowisku, przepisy dotyczące bezpieczeństwa wykorzystywane są jako kontrola ryzyka. Ramy prawne, w których wdrażane są przepisy, zostały opracowane w odpowiedzi na zagrożenia oraz kontrolę i nadzór nad przestrzeganiem regulacji, mając na uwadze dwa cele: zgodność z przepisami, ale co najważniejsze, weryfikację skutecznego działania w zakresie bezpieczeństwa.

6.9.5 W środowisku, w którym bezpieczeństwo realizowane jest w oparciu o wyniki działań, konieczne jest zdefiniowanie zestawu mierzalnych celów dla SSP i mierzalnych celów wydajności SMS w celu ustalenia czy obydwa systemy działają zgodnie z oczekiwaniami, poza zgodnością z przepisami. Wymierne cele i wskaźniki wydajności pozwalają na ocenę rzeczywistej wydajności działań istotnych dla bezpieczeństwa w kontekście istniejących organizacji kontroli, tak, aby niezbędne działania korygujące i zapobiegawcze mogły być podjęte, a zagrożenia utrzymane na poziomie najniższym z możliwych (ALARP).

6.9.6 Pojęcie akceptowalnego poziomu bezpieczeństwa związane z SSP i wydajności bezpieczeństwa z SMS to podstawowe składniki dla skutecznego działania zarówno SSP, jak i SMS. Stanowią one podstawę regulacji dla środowiska opartego na wydajności bezpieczeństwa, w celu monitorowania faktycznej realizacji SSP i faktycznych wyników realizowanych przez SMS, za zgodność z przepisami. Tylko poprzez tworzenie i pomiar poszczególnych celów w zakresie bezpieczeństwa i docelowej wydajności bezpieczeństwa – poprzez zapewnienie skutecznej realizacji SSP i skutecznego poziomu bezpieczeństwa SMS – możliwe jest osiągnięcie ciągłej poprawy wyników w zakresie SSP i SMS.

6.9.7 Oprócz zgodności z przepisami, wskaźniki bezpieczeństwa i cele bezpieczeństwa, wskaźniki realizacji/wydajności bezpieczeństwa i cele bezpieczeństwa, jakie mają zostać zrealizowane, stanowią wymierny sposób zapewnienia, i wykazania skuteczności odpowiednio SSP lub SMS. Dla państwa, jak również dla dostawców usług świadczących usługi lotnicze, zgodność z przepisami i regulacjami nadal leży u podstaw zarządzania bezpieczeństwem. Rysunki 6-8 i 6-9 opierają się na przykładach wskaźników bezpieczeństwa i celów bezpieczeństwa, wskaźników wydajności bezpieczeństwa, wskaźników docelowej wydajności i planów działań odpowiednio SSP i SMS, które zostały omówione w tym rozdziale w celu zilustrowania, gdzie, i w jaki sposób podejście oparte na normach i nakazach oraz podejście oparte na wynikach, czy inaczej mówiąc wykonaniu, wpisują się w SSP oraz SMS.

## *Wykonanie*

| | |
|---|---|
| **Ilościowe określenie celów bezpieczeństwa do osiągnięcia** | 1. Zredukować o (*wskazanie liczby)* liczbę / maksymalnie (*wskazanie liczby*) niezgodnych podejść (NCA) na pięciu lotniskach międzynarodowych w stosunku do (*wskazanie liczby*) przylotów w terminie do (*podanie daty*).<br>2. Zmniejszyć o (*wskazanie liczby*) liczbę / maksymalnie (*wskazanie liczby*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (*nazwa kraju*) w stosunku do (*wskazanie liczby*) operacji w terminie do (*podanie daty*).<br>3. **.....** |
| **Plan działań w stosunku do określonych celów** | 1. Wdrożenie procedur ciągłego zniżania (constant descent arrival – CDA). Opracowanie projektów graficznych procedur podejścia dla ustabilizowanego zbliżania.<br>2. Instalacja ASDE/X na pięciu międzynarodowych lotniskach (*nazwa kraju*).<br>3. … |
| **Wartości wskaźnika bezpieczeństwa** | 1. (*Wskazanie liczby)* niezgodnych podejść (NCA) na pięciu lotniskach międzynarodowych w stosunku do (*wskazanie liczby*) operacji.<br>2. (*Wskazanie liczby*) wtargnięć na drogi startowe kategorii B i C na pięciu lotniskach międzynarodowych (*nazwa kraju*) w stosunku do (*wskazanie liczby*) operacji.<br>3. … |

## *Norma*

| | |
|---|---|
| **Państwo** | Wymagana zgodność z wszystkimi normami międzynarodowymi, które mają zastosowanie. |

**Rys. 6-8. Krajowy program bezpieczeństwa (SSP) – Połączenie podejścia opartego na wykonaniu z podejściem nakazowym**

6.9.8 Podsumowując, zgodnie ze zharmonizowanymi normami oraz zalecanymi metodami i zasadami postępowaniami ICAO w zakresie zarządzania bezpieczeństwem:

a) Państwa ustanowią krajowy program bezpieczeństwa (State Safety Programme - SSP), w celu osiągnięcia akceptowalnego poziomu bezpieczeństwa (ALoS) w lotnictwie cywilnym.

b) Akceptowalny poziom bezpieczeństwa (ALoS), jaki ma zostać osiągnięty, ustalany jest przez państwo.

c) Dostawcy usług świadczący usługi lotnicze wdrożą SMS, który będzie:

1) identyfikował zagrożenia bezpieczeństwa;

2) zapewniał działania zaradcze w celu utrzymania poziomu bezpieczeństwa;

3) pozwalał na ciągłe monitorowanie i regularną ocenę działań oraz ich efektów podejmowanych na rzecz zachowania bezpieczeństwa;

4) miał na celu ciągłą poprawę całościowego funkcjonowania SMS.

## *Wykonanie*

| | |
|---|---|
| **Ilościowe określenie celów bezpieczeństwa do osiągnięcia** | 1. (*Wskazanie liczby*) zdarzeń związanych z wtargnięciem nieuprawnionych pojazdów na drogi kołowania w stosunku do (*wskazanie liczby*) operacji na pięciu lotniskach międzynarodowych (*nazwa kraju*) w terminie do (*podanie daty*).<br>2. (*Wskazanie liczby*) zdarzeń FOD na płycie lotniska w stosunku do (*wskazanie liczby*) operacji.<br>3. … |
| **Plan działań w stosunku do określonych celów** | 1. Szkolenia dla kierowców / instalacja specjalnego oznakowania.<br>2. Trzydniowy program inspekcji bezpośrednio na rampie.<br>3. … |
| **Wartości wskaźnika bezpieczeństwa** | 1. *(Wskazanie liczby)* zdarzeń związanych z wtargnięciem nieuprawnionych pojazdów na drogi kołowania na pięciu lotniskach międzynarodowych (*nazwa kraju*).<br>2. *(Wskazanie liczby)* zdarzeń FOD na płycie lotniska na pięciu lotniskach międzynarodowych (*nazwa kraju*).<br>3. … |

## *Norma*

| | |
|---|---|
| **Państwo** | Wymagana zgodność ze wszystkimi normami międzynarodowymi, które mają zastosowanie. |

**Rys. 6-9. SMS – Połączenie podejścia opartego na wykonaniu z podejściem nakazowym**

# Rozdział 7

# WPROWADZENIE DO SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM (SMS)

## 7.1 CEL I ZAWARTOŚĆ

Niniejszy rozdział opisuje podstawowe cechy systemów zarządzania bezpieczeństwem (SMS) i omawia rolę i znaczenie prawidłowego opisu systemu (opis systemu) oraz dokonania analizy luk w systemie przed rozpoczęciem procesu jego wdrażania. Rozdział omawia również zależność pomiędzy systemami zarządzania bezpieczeństwem i systemami zarządzania jakością (QMS). W rozdziale omówione są następujące zagadnienia:

a) Koncepcje wprowadzające;

b) Cechy SMS;

c) Opis systemu;

d) Analiza luk w systemie;

e) SMS i QMS;

f) SSP/SMS oraz proces badania wypadków;

g) Integracja systemów zarządzania;

h) Wyjaśnienie pojęć;

i) Różnice pomiędzy sloganami związanymi z bezpieczeństwem a zasadami bezpieczeństwa.

## 7.2 KONCEPCJE WPROWADZAJĄCE

7.2.1 Zarządzanie systemem bezpieczeństwa można porównać do skrzynki z narzędziami. Jest to skrzynka zawierająca narzędzia, których organizacja lotnicza potrzebuje do kontrolowania ryzyka bezpieczeństwa będącego konsekwencją zagrożeń, którym musi sprostać podczas realizacji usług stanowiących jej działalność handlową. W wielu przypadkach sama organizacja stwarza zagrożenia podczas realizacji usługi. Należy pamiętać, że zarządzanie systemem bezpieczeństwa samo w sobie nie jest ani narzędziem ani procesem. Zarządzanie systemem bezpieczeństwa jest skrzynką z narzędziami, w której znajdują się i są chronione narzędzia wykorzystywane w dwóch podstawowych procesach zarządzania bezpieczeństwem (identyfikacja zagrożeń i zarządzanie ryzykiem). Zarządzanie systemem bezpieczeństwa jest jak skrzynka z narzędziami o wielkości i złożoności odpowiedniej dla wielkości i złożoności organizacji.

7.2.2 Jako skrzynka z narzędziami (Rys. 7-1), zarządzanie bezpieczeństwem zapewnia, że w przypadku konieczności zidentyfikowania zagrożenia lub zarządzania ryzykiem:

a) odpowiednie dla wykonania zadania narzędzie jest dostępne do wykorzystania przez organizację;


**Rysunek 7-1. SMS — Skrzynka z narzędziami**

b) narzędzia i zadania są odpowiednio ze sobą powiązane;

c) narzędzia są współmierne do potrzeb i ograniczeń organizacji;

d) bez zbędnego wysiłku i straty czasu w skrzynce bardzo łatwo można znaleźć narzędzie.

Taka perspektywa jest ważna, gdyż zarządzanie systemem bezpieczeństwa stanowi tylko skorupę ochronną, która zapewnia prawidłowe i aktualne składowanie, dostępność i możliwość wykorzystania narzędzi potrzebnych dla wprowadzenia w organizacji szczególnych procesów zarządzania bezpieczeństwem. Bez odpowiednich narzędzi w skrzynce, zarządzanie systemem bezpieczeństwa jest tylko pustym pojęciem.

7.2.3 Rozdział 3, w swoim końcowym podsumowaniu, przedstawia w ogólnych zarysach kilka charakterystycznych lub wyróżniających się właściwości zarządzania bezpieczeństwem. Jedną z istotnych właściwości jest to, że zarządzanie systemem bezpieczeństwa nie jest ograniczone do jednej konkretnej dziedziny działalności organizacji, zazwyczaj najbardziej spektakularnej (np. operacji lotniczych przewoźnika), która może generować zagrożenia. Zarządzanie systemem bezpieczeństwa obejmuje całą działalność operacyjną organizacji. Zakres zarządzania systemem bezpieczeństwa obejmuje większość działalności organizacji, a na pewno działania operacyjne, które wspomagają świadczenie usług i mają w sobie potencjał do generowania zagrożeń. Zakres zarządzania systemem bezpieczeństwa bezpośrednio obejmuje operacje, obsługi, naprawy, usługi wspomagające, szkolenie i kontrolę oraz inną działalność operacyjną. Pośrednio, zakres zarządzania systemem bezpieczeństwa uwzględnia, o ile ma to zastosowanie i odnosi się do świadczonej usługi; inne działania organizacyjne, które wspomagają działalność operacyjną, takie jak finansowe, kadrowe i prawne, jak omówiono w rozdziale 3.

7.2.4 Zarządzanie bezpieczeństwem musi zaczynać się na poziomie wyższego szczebla kierowniczego. Nie jest to stwierdzenie retoryczne ani filozoficzne, ale oparte na bardzo solidnych/konkretnych racjach. Tak jak każda funkcja działalności podstawowej, zarządzanie bezpieczeństwem jako istotna funkcja działalności podstawowej, wymaga środków finansowych. Przyznanie odpowiednich środków finansowych jest ewidentnie zadaniem kierownictwa, gdyż ma ono odpowiednią władzę i jest odpowiedzialne za rozdzielanie tych środków. Jeżeli kierownictwo nie wie, jaka jest rola i cele zarządzania systemem bezpieczeństwa w organizacji lub nie jest zaangażowane w jego tworzenie na odpowiednim poziomie nie będzie zdawać sobie sprawy ze stopnia zagrożenia, jakie stwarza ryzyko bezpieczeństwa dla organizacji. Bez odpowiedniej wiedzy przydzielone środki finansowe mogą okazać się za małe dla faktycznych potrzeb. Innymi słowy, najprawdopodobniej pojawi się omówiony w rozdziale 3 „dylemat dwóch P", który pozostanie nierozwiązany.

7.2.5 Celem zarządzania systemem bezpieczeństwa jest ciągłe ulepszanie poziomu bezpieczeństwa organizacji. Zgodnie z istotą zarządzania bezpieczeństwem, stanowiącą funkcję działalności podstawowej, zarządzanie bezpieczeństwem wymaga ciągłej, codziennej identyfikacji zagrożeń, zbierania informacji i analiz, zakładania ryzyka i wprowadzania środków jego łagodzenia. Nie ma żadnego konkretnego punktu, w którym zarządzanie systemem bezpieczeństwa zatrzymuje się lub zwalnia. Zarządzanie bezpieczeństwem jest stałą, nigdy niekończącą się operacją, której celem jest utrzymanie, i na ile to możliwe, poprawianie poziomów bezpieczeństwa, które są współmierne ze strategicznymi celami organizacji i wspierającymi funkcjami działalności podstawowej. W tym rozumieniu pojęcie zarządzania bezpieczeństwem jest całkowicie inne od tradycyjnego pojęcia badania wypadku, kiedy już po zdarzeniu, w wyniku dochodzenia, wyciągano wnioski dotyczące bezpieczeństwa, które upowszechniano w celu zapobieżenia podobnym wypadkom w przyszłości. Zarządzanie systemem bezpieczeństwa aktywnie poszukuje zagrożeń, ciągle ocenia ryzyka bezpieczeństwa celem zapanowania nad nimi zanim wypadek będzie miał miejsce.

7.2.6 Z bardzo konkretnych powodów wszyscy uczestnicy sektora lotniczego mają swój udział w zarządzaniu bezpieczeństwem. Bardzo ważnym jest zaangażowanie uczestników sektora lotniczego dla zapewnienia, że ich wkład i wiedza związane z podejmowaniem decyzji dotyczących ryzyka bezpieczeństwa są uwzględniane przed ich podjęciem.

7.2.7 Ponadto, uwzględniając szeroki zasięg działania SMS, niezmiernie istotny jest wkład różnych działów w proces podejmowania decyzji dotyczących ryzyka bezpieczeństwa. Poniżej przedstawiona została lista interesariuszy, którzy mogą zostać wezwani w celu wsparcia lub uczestniczenia w procesie podejmowania decyzji dotyczących ryzyka bezpieczeństwa:

a) pracownicy sektora lotniczego;

b) właściciele i użytkownicy statków powietrznych;

c) producenci;

d) władze lotnicze;

e) zrzeszenia handlu i przemysłu;

f) podmioty świadczące usługi lotnicze na skalę regionalną;

g) zrzeszenia zawodowe i federacje;

h) międzynarodowe organizacje lotnicze;

i) agencje badania wypadków;

j) społeczeństwo korzystające z transportu lotniczego.

7.2.8 Interesariusze mogą wspierać osoby podejmujące decyzje w organizacji przez dopilnowanie, że wymiana informacji o rozważanych zagrożeniach/ryzykach bezpieczeństwa odbywa się z wyprzedzeniem i w sposób uczciwy, obiektywny i zrozumiały. Aby informacje o bezpieczeństwie były wiarygodne, muszą być zgodne z faktami, z wcześniejszymi oświadczeniami kierownictwa i wiadomościami od innych władz lotniczych. Wiadomości muszą być wyrażane w sposób zrozumiały dla udziałowców.

### 7.3 CECHY SMS

7.3.1 Trzy cechy charakteryzujące SMS:

a) systematyczny;

b) proaktywny;

c) jawny.

7.3.2 SMS jest usystematyzowany, gdyż czynności w zakresie zarządzania bezpieczeństwem są wykonywane zgodnie z wcześniej ustalonym planem oraz są konsekwentnie stosowane w całej organizacji. Długoterminowy plan utrzymywania pod kontrolą ryzyk bezpieczeństwa mogących stanowić konsekwencję zagrożeń jest opracowywany, zatwierdzany, wdrażany i stosowany na bieżąco w trybie ciągłym. Działania SMS ze względu na swój systematyczny i strategiczny charakter są ukierunkowane na stopniowe, ale stałe jego usprawnianie, w przeciwieństwie do gwałtownej, dramatycznej zmiany. Systematyczny charakter SMS również prowadzi do koncentrowania się raczej na procesach niż skutkach. Aczkolwiek skutki zdarzeń (tj. zdarzenia niekorzystne) są należycie rozważane dla wyciągnięcia wniosków wspomagających monitorowanie ryzyka bezpieczeństwa, to SMS koncentruje się głównie na wyszukiwaniu, podczas rutynowych czynności operacyjnych (procesów), w które zaangażowana jest organizacji przy realizacji usług, zagrożeń stanowiących zwiastun wydarzeń.

7.3.3 SMS jest proaktywny, ponieważ kształtuje się w oparciu o podejście, które kładzie nacisk na zapobieganie zdarzeniom poprzez identyfikację zagrożeń oraz nadzorowanie i wprowadzanie środków łagodzenia ryzyka, zanim wystąpi zdarzenie zagrożone ryzykiem. Obejmuje to strategiczne planowanie, które stara się utrzymać ryzyka bezpieczeństwa pod stałą kontrolą organizacji zamiast angażować się w działania naprawcze po doświadczeniu niekorzystnego zdarzenia, a następnie przejście w „tryb uśpienia” do kolejnego niekorzystnego zdarzenia, kiedy to znowu przywraca się działania naprawcze. W celu utrzymania skutecznej identyfikacji zagrożenia, prowadzony jest ciągły monitoring działań operacyjnych niezbędnych dla świadczenia usług. To z kolei pozwala na zbieranie danych dotyczących bezpieczeństwa odnośnie zagrożeń oraz podejmowanie i monitorowanie decyzji związanych z zagrożeniem w oparciu o dane będące w posiadaniu organizacji w przeciwieństwie do formułowania decyzji związanych z ryzykiem bezpieczeństwa w oparciu o opinie lub jeszcze gorzej, w oparciu o niechęć lub uprzedzenia.

7.3.4 I na koniec, SMS jest jawny, ponieważ wszystkie czynności w zakresie zarządzania bezpieczeństwem są udokumentowane, widoczne, a w związku z tym istnieje możliwość obrony danych założeń. Czynności w zakresie zarządzania bezpieczeństwem i wynikająca z tego wiedza o jego zarządzaniu w organizacji są formalnie odnotowane w oficjalnych dokumentach, do których każdy ma dostęp. W związku z tym "archiwum bezpieczeństwa" omawiane w rozdziale 4 odgrywa podstawową rolę dla zapewnienia, że czynności w zakresie zarządzania bezpieczeństwem i związana z tym wiedza są udokumentowane w formalnych strukturach organizacyjnych, a nie pozostają do dyspozycji tylko dla pojedynczych osób. Organizacja, która dopuszcza do sytuacji, w której czynności w zakresie zarządzania bezpieczeństwem i związana z tym wiedza nie jest ogólnodostępna stawia się bardzo delikatnej sytuacji, jeżeli chodzi o zachowania ciągłości działań z zakresu zarządzania bezpieczeństwem i stosownej wiedzy.

### 7.4 OPIS SYSTEMU

7.4.1 Opis systemu jest pierwszym warunkiem dla przygotowania SMS. W rozdziale 2 omówiono współdziałanie pomiędzy ludźmi, kontekst i bezpieczeństwo w środowisku lotniczym. Sugeruje się, że słabości w systemie bezpieczeństwa można znaleźć tam, gdzie pojawia się niedopasowanie we współdziałaniu pomiędzy ludźmi oraz innymi elementami obszaru operacyjnego, w którym ludzie realizują świadczenie/dostarczanie usług *(service-delivery activities).* Potencjalną słabość bezpieczeństwa, będącą konsekwencją współdziałania pomiędzy ludźmi i innymi elementami obszaru operacyjnego można scharakteryzować w kategoriach zagrożeń, które posiadają identyfikowalne i kontrolowalne elementy. Zagrożenia stanowią unikalne elementy systemów produkcyjnych, a najwięcej zagrożeń uwalnia swój niszczący potencjał wskutek interakcji operacyjnej z różnymi jego elementami.

7.4.2 Poniżej opisano bardzo prosty przykład. Paliwo stanowi składnik systemu lotniczego i podobnie, jak inne źródła energii, stanowi zagrożenie. W czasie składowania w podziemnych zbiornikach, niedotykane, niszczące paliwo stanowi bardzo niski poziom zagrożenia. Statki powietrzne również są składnikami systemu lotniczego. Ludzie muszą wlać paliwo do statków powietrznych. Podczas operacji tankowania paliwa wykonywanej przez ludzi (interakcja operacyjna niezbędna dla wykonana usługi dostawy), niszczący potencjał

paliwa, jako zagrożenie znacząco wzrasta. W tym przypadku stosuje się procedury tankowania, aby operację tankowania, stanowiącą zagrożenie, wprowadzić pod kontrolę organizacji. Procedury te oparte są na identyfikacji i kontroli elementów stanowiących zagrożenie. Identyfikacja elementów stanowiących zagrożenie i w dużym stopniu ich kontrola oparta jest na opisie systemu co stanowi pierwszy i podstawowy krok.

7.4.3 Przykład wykorzystany w rozdziale 2 wyjaśniający współzależność pomiędzy ludźmi, kontekstem i bezpieczeństwem w środowiskach lotniczych jest również przydatny dla objaśnienia opisu systemu.

7.4.4 Rysunek 7-2 przedstawia środowisko, w którym ma miejsce świadczenie usług. Wspomnianą usługą jest dostawa przez ludzi (jaskiniowców) małych paczek na drugą stronę gór. Kombinacja zaangażowanych w dostawę osób, użyte przez nich narzędzia i środki oraz cechy środowiska stanowią kontekst operacyjny, w którym dostarczanie usług będzie miało miejsce. System, o którym mowa to system społeczno-techniczny (tzn. system, który uwzględnia ludzi i technikę) dla dostarczenia paczek. Ponieważ słabości w systemie bezpieczeństwa są charakteryzowane, jako zagrożenia, które można znaleźć w niedopasowaniu współdziałania pomiędzy ludźmi oraz innymi elementami obszaru operacyjnego, w którym ludzie realizują swoje usługi-dostawy, pierwszym krokiem dla zidentyfikowania takiego niedopasowania jest przygotowanie opisu systemu zawierającego jego elementy i współdziałanie między nimi.


**Rysunek 7-2. Opis systemu**

7.4.5 Wykorzystując model SHEL opis systemu w odniesieniu do jego elementów i ich współdziałania, omówiony w rozdziale 2, wyglądałby następująco: funkcją systemu społeczno-technicznego jest dostawa paczek. Funkcja ta jest współzależna od innych systemów: topograficznego, pogodowego i dzikiej fauny. Występuje również system socjalny: ludzie. Należy rozważyć możliwości człowieka, które stanowią fundament dla funkcjonowania systemu: jaki będzie skutek spotkania ludzi z lwami, jak ludzie zareagują na góry, pogodę? W systemie występują elementy konstrukcyjne: droga przez góry, znaki ostrzegawcze, a także elementy oprogramowania: dokumenty, procedury i szkolenie przeprowadzające ludzi przez wykonywaną operację oraz współdziałanie z systemem (jak postąpić z lwami, jak pokonać zakręty na drodze, jak ochronić się przed pogodą), w tym samym czasie zapewniając wykonanie dostawy (paczki muszą być dostarczone na drugą stronę góry w stanie nienaruszonym).

7.4.6 W zakresie formalnym i technicznym opis sytemu w lotnictwie powinien zawierać jak niżej:

a) współzależność między systemami w systemie transportu lotniczego;

b) funkcje systemu;

c) rozważania o możliwościach człowieka koniecznych dla funkcjonowania systemu;

d) elementy konstrukcyjne systemu;

e) elementy oprogramowania systemu, włącznie z odnośnymi procedurami, które definiują wytyczne dla funkcjonowania i stosowania systemu;

f) środowisko operacyjne;

g) zakontraktowane i kupione produkty i usługi.

7.4.7 Dodatek 1 do niniejszego rozdziału zawiera wytyczne dla opisania systemu.

### 7.5 ANALIZA LUK W SYSTEMIE

7.5.1 Pierwszym krokiem do zidentyfikowania słabości systemu bezpieczeństwa, wymienionych jako zagrożenia we współdziałaniu ludzi z innymi elementami systemu stanowi opis systemu. Gdy system jest już opisany w zakresie jego elementów i występujących współzależności, kolejnym krokiem jest omówienie słabości systemu bezpieczeństwa wyszczególnionych jako zagrożenia we współdziałaniu ludzi z innymi elementami systemu wykonując analizę już obecnych jego zasobów. Analiza ma dwa założenia. Pierwsze to zidentyfikowanie ewentualnych niedopasowań we współdziałaniu różnych elementów zidentyfikowanych w opisie systemu. Te niedopasowania stanowią słabości systemu bezpieczeństwa. Drugim założeniem jest zidentyfikowanie wszystkich dodatkowych zasobów potrzebnych dla wygładzenia nierównych płaszczyzn współdziałania w celu wsparcia osób zaangażowanych w realizację usług i zadań w sposób bezpieczny i skuteczny. Analiza ta znana jest jako analiza przyczyn powstawania luk w systemie.

7.5.2 Z perspektywy SMS analiza przyczyn powstawania luk w systemie jest zasadniczo analizą porównawczą już istniejących w organizacji zasad bezpieczeństwa w odniesieniu do tych, które są wymagane do funkcjonowania SMS. Analiza przyczyn powstawania luk w systemie jest ważna, ponieważ w organizacji mogą już istnieć podstawowe struktury organizacyjne potrzebne dla rozpoczęcia opracowywania SMS: konieczność stworzenia SMS od podstaw wystąpi niezwykle rzadko, gdyż różne czynności związane z SMS w większości organizacji będą już funkcjonować. Przy rozbudowie SMS należy wykorzystać i nadbudować istniejące struktury organizacyjne.

7.5.3 Wracając do rys. 7-2 i pamiętając, że świadczona przez system usługa to dostawa na drugą stronę gór małych paczek, prosta analiza przyczyn powstawania luk w systemie przytoczona jest jako przykład. Wiodącym pytaniem w analizie powinno być: czy personel operacyjny (w tym przypadku jaskiniowcy), który faktycznie ma zrealizować usługę jest odpowiednio wyposażony w niezbędne zasoby do jej wykonania? Odpowiedź na pytanie musi omawiać zarówno zagadnienie bezpieczeństwa (tzn. czy pracownicy są odpowiednio wyposażeni, aby bezpiecznie zrealizować usługę?) oraz skuteczność (tzn. czy pracownicy są odpowiednio wyposażeni, aby skutecznie zrealizować usługę?).

7.5.4 Omówiony w rozdziale 2 model SHEL jest przydatnym narzędziem do udzielenia odpowiedzi na pytanie i przeprowadzenie analizy przyczyn powstawania luk w systemie. Jaskiniowiec reprezentuje Czynnik ludzki (L) [ang. „Liveware"]. Droga, znak STOP, znak prędkości i tunel niedaleko szczytu stanowią Sprzęt (H) [ang. „Hardware"]. Drzewa, lwy, góry i chmury to Środowisko (E) [ang. „Environment"]. Aczkolwiek niewidoczne szkolenie, które przeszedł jaskiniowiec oraz procedury i instrukcje, których musi przestrzegać, aby zrealizować usługę to Oprogramowanie (S) [ang. „Software"]. Jak pokazano na rys. 7-3 analiza przyczyn powstawania luk w systemie przy porównaniu z rys. 7-2 mogłaby doprowadzić do następujących wniosków:

a) Jaskiniowiec, okrężną i prawdopodobnie nierówną drogą musi boso podróżować przez góry. Może w związku z tym pokaleczyć stopy i doznać upadku (bezpieczeństwo) i/lub posuwać się bardzo wolno, a więc opóźnić dostawę paczek (skuteczność). Analiza przyczyn powstawania luk w systemie sugeruje, że zapewnienie obuwia byłoby ważnym zagadnieniem do omówienia jako niedopasowanie we współzależności jaskiniowca (L) od drogi (H).

b) Chmury mogą stanowić zagrożenie wystąpienia deszczu i piorunów. Zapewnienie nakrycia głowy chroniłoby jaskiniowca i jednocześnie zrównoważyłoby niedopasowanie we współzależności jaskiniowca (L) od chmur (E).


**Rys. 7-3. Analiza luk w systemie**

c) Lwy stanowią ewidentne zagrożenie dla jaskiniowca, jak i dla realizacji usługi. Znak STOP jest już zasobem występującym w systemie, którego zadaniem jest ostrzeżenie jaskiniowca o zagrożeniu/ryzyku (tzn. wejście w szczególnie niebezpieczną strefę). Mimo wszystko, narzędzie do samoobrony byłoby odpowiednim, dodatkowym zasobem. Zapewnienie jaskiniowcowi dzidy zrównoważyło niedopasowanie we współzależności jaskiniowca (L) od lwów (E).

d) Dodatkowo do znaku STOP, namalowanie na drodze żółtych „wstrzymujących" pasów tuż przed wejściem w szczególnie niebezpieczną strefę zwiększyłoby czujność jaskiniowca i skierowałoby jego uwagę na lwy, stanowiąc dodatkowe, obok dzidy, narzędzie w celu zrównoważenia niedopasowania we współzależności jaskiniowca (L) od lwów (E).

e) Jaskiniowiec nie posiada żadnego wyposażenia do transportu małych paczek, a musi mieć wolne ręce w celu trzymania dzidy oraz dla utrzymania lepszej równowagi i stabilności podczas podróży nierówną drogą górską. Plecak do przenoszenia paczek byłby dodatkowym zasobem równoważącym niedopasowanie we współzależności jaskiniowca (L) od drogi (H).

f) Na początku drogi znajduje się znak prędkości, który nie przekazuje jednoznacznej wiadomości o warunkach na zbliżającej się drodze. Wyraźny znak ostrzegawczy poświęcony tylko dzidzie byłby dodatkowym zasobem równoważącym niedopasowanie we współzależności jaskiniowca (L) od drogi (E).

g) Nie ma żadnego ostrzeżenia, że przejście przez szczyt góry prowadzi przez tunel. Znak ostrzegawczy byłby dodatkowym zasobem równoważącym niedopasowanie na styku jaskiniowca (L) od drogi (E).

7.5.5 Tak więc analiza przyczyn powstawania luk w systemie, ujawnia istniejące już zasoby i struktury związane z bezpieczeństwem. Odsłania słabości systemu bezpieczeństwa, wyszczególnione jako zagrożenia, a będące konsekwencją współzależności występującej pomiędzy ludźmi a innymi elementami kontekstu operacyjnego. Ujawnia również dodatkowe potrzeby w celu podwyższenia odporności operacyjnej na ryzyka bezpieczeństwa.

7.5.6 Gdy analiza przyczyn powstawania luk w systemie jest kompletna i w pełni udokumentowana, to zasoby i struktury, które zostały zidentyfikowane jako brakujące lub niepełne, stworzą wraz z już istniejącymi, podstawę wdrożenia SMS. Organizacje mogą ukształtować plan wdrożenia SMS zgodnie z własnymi potrzebami, ale dla ułatwienia czytania i śledzenia zaleca się format rozkładanego arkusza, tablicy Gantt lub MS Project. Każdy element zostanie poddany ocenie dla stwierdzenia w jaki sposób organizacja będzie tworzyć lub modyfikować swoją politykę, procedury lub procesy, aby wprowadzić wymagane elementy i części SMS. Dodatek 2 do niniejszego rozdziału zawiera przykład analizy przyczyn powstawania luk w systemie wraz z sugerowanymi pytaniami do usługodawców ułatwiającymi organizacji określenie braków po opisaniu własnego systemu.

### 7.6 SMS i QMS

7.6.1 Zarządzanie jakością już od dawna funkcjonuje w wielu segmentach systemu lotniczego. Wiele organizacji lotniczych wdrożyło i od wielu lat korzysta z kontroli jakości (QC) i/lub zapewnienia jakości (QA).

7.6.2 Program zapewnienia jakości definiuje i określa politykę jakości organizacji i jej założenia. Polityka jakości zapewnia, że wszystkie elementy konieczne dla usprawnienia skuteczności i obniżenia ryzyka związanego ze świadczonymi usługami są na miejscu. Prawidłowe wdrożenie programu zapewnia wymaganą jakość i sprawia, że procedury są stosowane konsekwentnie i zgodnie ze stosownymi wymaganiami. Problemy są identyfikowane i rozwiązywane. Dzięki temu organizacja na bieżąco analizuje i usprawnia swoje procedury, produkty i usługi. System zapewnienia jakości musi identyfikować problemy i usprawniać procedury w celu spełnienia celów korporacyjnych.

7.6.3 Zastosowanie zasad QA w procesach zarządzania bezpieczeństwem pomaga zapewnić, że w systemie podjęto wymagane środki bezpieczeństwa dla wsparcia organizacji w osiągnięciu swoich założeń dotyczących bezpieczeństwa. Jednakże system zapewnienia jakości sam w sobie, zgodnie z sugestią zawartą w dogmacie jakości, nie może „zapewniać bezpieczeństwa”. Włączenie zasad systemu zapewnienia jakości i koncepcji do SMS, który jest elementem zapewnienia jakości (omówionym w rozdziale 9) wspomaga organizację w normalizowaniu niezbędnych procesów koniecznych dla zrealizowania dalekosiężnego celu. Celem tym jest zarządzanie ryzykiem bezpieczeństwa wynikającym ze skutków zagrożeń, którym organizacja musi sprostać przy wykonywaniu czynności związanych z realizacją usług.

7.6.4 Zasady systemu zapewnienia jakości uwzględniają procedury monitorowania wszystkich dziedzin działalności organizacji, w tym takich elementów jak:

a) projektowanie i dokumentowanie procedur (np. SOPs);

b) metody inspekcji i sprawdzania;

c) monitorowanie sprzętu i operacji;

d) audyty wewnętrzne i zewnętrzne;

e) monitorowanie podjętych działań naprawczych;

f) stosowanie odpowiednich analiz statystycznych, jeżeli wymagane.

7.6.5 Kilka organizacji lotniczych połączyło swoje systemy kontroli i zapewnienia jakości w tzw. systemy zarządzania jakością (QMS). Aktualnie stosowanych jest i uznanych na skalę międzynarodową szereg standardów dotyczących zapewniania jakości. Standardy zależą od wielkości, złożoności i produktu organizacji. Norma ISO 9001-2000, jest np. jednym z międzynarodowych standardów przygotowanych przez ISO i stosowanych przez wiele organizacji do wdrożenia wewnętrznego systemu zarządzania jakością. Stosowanie takich systemów również gwarantuje, że dostawcy i kontrahenci mają na miejscu odpowiednie systemy zarządzania jakością.

7.6.6 Mając na uwadze długą historię obecności kontroli i zapewnienia jakości w lotnictwie, a stosunkową „młodość" SMS i fakt, że specyficzne procesy SMS kształtują się poprzez zasady jakości, to potencjał niewłaściwego postrzegania i nieporozumień dotyczących związku pomiędzy SMS a QMS jest rzeczywisty. W związku z tym, konieczne jest zdefiniowanie tego związku z perspektywy synergii, a nie przeciwstawienia oraz względnego udziału SMS i QMS w osiąganiu całościowych celów organizacji, w tym celów związanych z bezpieczeństwem.

7.6.7 Można powiedzieć, że SMS i QMS łączy wiele wspólnych cech:

a) muszą być zaplanowane i zarządzane;

b) zależne są od rozmiaru i monitorowania;

c) dotyczą każdej funkcji, procesu i osoby w organizacji;

d) dążą do ciągłego usprawniania.

7.6.8 Ponieważ SMS i QMS łączy wiele wspólnych cech, może pojawić się tendencja, która zakłada, że organizacja, która stworzyła i zarządza systemem zarządzania jakością nie potrzebuje SMS lub już go ma. Pomimo, że SMS i QMS łączy wiele wspólnych cech to występują pomiędzy nimi zasadnicze różnice i niedociągnięcia w zakresie skuteczności co do samodzielnego zrealizowania przez QMS dalekosiężnego celu, którym jest zarządzanie ryzykiem bezpieczeństwa wynikającym ze skutków zagrożeń, którym organizacja musi stawić czoła przy wykonywaniu czynności związanych z realizacją usług.

7.6.9 Zarządzanie jakością wprowadzono w latach sześćdziesiątych XX wieku, kiedy wiedza o możliwościach człowieka, czynnikach organizacyjnych i ich wpływ na bezpieczeństwo była znacznie mniej rozbudowana niż dzisiaj. Tak więc, niezależnie od modyfikacji i stałego aktualizowania, zarządzanie jakością jest mniej skuteczne, jeżeli identyfikowane są wyłącznie problemy poważne lub z poważnymi następstwami, takie jak przebieg ukrytej awarii, co w konsekwencji może doprowadzić do katastrofy. Ponadto biurokracja związana z audytowaniem i uzyskaniem formalnej akredytacji jakościowej z dużym prawdopodobieństwem może stać się celem samym w sobie: dążenie do powieszenia baneru z akredytacją ISO nad wejściem do siedziby firmy odciągnie organizację od tworzenia praktyk związanych z bezpieczeństwem i rozproszenia uwagi, która mogłaby być skupiona na bezpieczeństwie.

7.6.10 SMS koncentruje się na możliwościach człowieka. Czynniki ludzkie i organizacyjne oraz techniki zarządzania jakością i procesy mają swój udział w uzyskaniu satysfakcji w obszarze bezpieczeństwa. Celem SMS jest zidentyfikowanie ryzyka bezpieczeństwa, któremu organizacja musi sprostać i które w wielu przypadkach sama generuje podczas realizacji usług oraz wprowadzania kontroli nad ryzykiem bezpieczeństwa będącego konsekwencją tych zagrożeń. Ogólnie mówiąc, pierwszy imperatyw założenia – identyfikacja zagrożenia – jest realizowany przez element zarządzania ryzykiem SMS (omawiany w rozdziale 9), który oparty jest na zasadach i praktykach zarządzania bezpieczeństwem. Drugi imperatyw – sprowadzanie ryzyka, pod kontrolę organizacji – jest realizowany przez element zapewnienia bezpieczeństwa SMS (również omawiany w rozdziale 9), a oparty na połączeniu zasad i praktyk zarządzania bezpieczeństwem.

7.6.11 Krótko mówiąc SMS różni sie od QMS następującymi cechami:

a) SMS koncentruje się na bezpieczeństwie, ludzkich i organizacyjnych aspektach organizacji (tzn. zadawalające bezpieczeństwo); podczas gdy

b) QMS koncentruje się na produktach i usługach świadczonych przez organizację (tzn. zadowolenie klienta).

7.6.12 Po ustaleniu cech wspólnych i różnic pomiędzy SMS i QMS istnieje możliwość ustalenia współzależności między systemami. Należy stanowczo podkreślić, że ta współzależność jest wzajemna i można ją podsumować następująco:

a) SMS jest w części skonstruowany w oparciu o zasady QMS;

b) SMS musi uwzględniać zarówno politykę bezpieczeństwa, jak i jakości oraz stosowne praktyki;

c) Połączenie zasad jakości, polityki i praktyk w zakresie dotyczącym SMS powinno być ukierunkowane na wspieranie zarządzania bezpieczeństwem.

7.6.13 Ustanowienie uzupełniającej się współzależności między SMS a QMS prowadzi do wzajemnie uzupełniającego się uczestniczenia w osiąganiu celów organizacji związanych z bezpieczeństwem:

a) Wynikiem SMS jest opracowanie i wdrożenie procesów i procedur w organizacji umożliwiających zidentyfikowanie ryzyka bezpieczeństwa i jego skutków oraz wprowadzenie ryzyka związanego z operacjami lotniczymi pod kontrolę organizacji;

b) Włączenie QMS do SMS zapewnia podejście strukturalne do monitorowania prawidłowości działania lub konieczności usprawnienia procesów i procedur umożliwiających zidentyfikowanie ryzyka bezpieczeństwa i jego skutków oraz wprowadzenie ryzyka związanego z operacjami lotniczymi, pod kontrolę organizacji.

7.6.14 Należy tu podkreślić, że SARPs ICAO zawarte w Załącznikach 1, 6, 8, 11 i 14 omówione w rozdziale 6 ograniczają się do SMS. W wymienionych Załącznikach nie ma żadnych wymagań ICAO dotyczących QMS, z wyjątkiem jednostkowego wymagania dla zatwierdzonych organizacji obsługowych (AMO) w Załączniku 6, Część I, Rozdział 8.

## 7.7 SSP/SMS ORAZ PROCES BADANIA WYPADKU

7.7.1 Podobnie jak powiązania pomiędzy SMS i QMS, powiązania pomiędzy SSP i SMS a procesem badania wypadku oraz rolą jaką odgrywa proces badania wypadku w środowisku zarządzania bezpieczeństwem, stanowi temat do dyskusji. Podczas gdy dyskusje głównie koncentrują się na powiązaniach pomiędzy SMS a procesem badania wypadku, niewątpliwie SSP również musi być częścią tejże dyskusji. Podobnie jak powiązania pomiędzy SMS i QMS, trudno jest określić czy powiązania pomiędzy SSP/SMS a procesem badania wypadku całkowicie się uzupełniają i wzajemnie na siebie oddziałują. Badanie wypadku jest istotnym narzędziem w procesie zarządzania bezpieczeństwem.

7.7.2 Zgodnie z procesem zarządzania bezpieczeństwem, codzienne czynności związane z zarządzaniem bezpieczeństwem, stanowiące kolejny proces w organizacji, jak omówiono w rozdziale 3, są dostarczane przez SSP lub SMS danej organizacji. Wypadek (lub poważny incydent) wskazuje na całkowitą niewydolność SSP lub SMS (lub obu) jako systemów zarządzających, kierujących czynnościami niezbędnymi dla zarządzania bezpieczeństwem kolejno w Państwie lub organizacji. Gdy wystąpi taka całkowita niewydolność uruchamiany jest proces badania wypadku w celu znalezienia przyczyn nieskuteczności działań związanych z zarządzaniem bezpieczeństwem i uruchomienia działań zapobiegających powtórzeniu się takiej sytuacji. Zatem w środowisku zarządzania bezpieczeństwem, proces badania wypadku spełnia bardzo istotną rolę. Jest ostatnim w systemie lotniczym „strażnikiem" chroniącym bezpieczeństwo, który uruchamia się, gdy zawiodły wszystkie zabezpieczenia, bariery, kontrole i przeciwdziałania systemu bezpieczeństwa.

## 7.8 INTEGRACJA SYSTEMÓW ZARZĄDZANIA

7.8.1 Organizacje lotnicze często są określane mianem „ system systemów". Jest to spowodowane tym, że organizacje lotnicze muszą opracować, wdrożyć i zarządzać wieloma różnymi systemami zarządzania, aby sprostać swoim założeniom produkcyjnym poprzez świadczenie usług. Typowymi systemami zarządzania, którymi organizacja będzie musiała kierować są:

a) system zarządzania jakością (QMS);

b) system zarządzania środowiskiem (EMS);

c) system zarządzania bezpieczeństwem i higiena w pracy (OHSMS);

d) system zarządzania bezpieczeństwem (SMS);

e) system zarządzania ochroną (SEMS).

7.8.2 W lotnictwie cywilnym pojawiła sie tendencja do łączenia wszystkich tych zróżnicowanych systemów zarządzania. Takie działanie ma wyraźne zalety:

a) ograniczenie powielania pracy, a więc obniżenie kosztów;

b) zmniejszenie ogólnego ryzyka organizacji i wzrost rentowności;

c) zrównoważenie potencjalnie sprzecznych celów;

d) zlikwidowanie potencjalnie sprzecznych obowiązków i zależności;

e) rozproszenie systemów władzy.

7.8.3 Istnieją jednak różne sposoby integrowania tych systemów, a szczególnie połączenia SMS z innymi systemami zarządzania. Należy zachęcać organizacje lotnicze do integrowania swoich systemów zarządzania jakością, ochroną, bezpieczeństwem, higieną pracy i ochroną środowiska. Integracja ta znajduje się jednak obecnie poza zakresem zharmonizowanych SARPs ICAO dotyczących zarządzania bezpieczeństwem oraz niniejszego podręcznika.

## 7.9 WYJAŚNIANIE POJĘĆ

Istotne jest wypracowanie jednolitego rozumienia terminologii dotyczącej innych czynności związanych z zarządzaniem bezpieczeństwem będących w gestii podmiotów lotniczych i/lub nadzorujących władz lotniczych. Użyte w niniejszym podręczniku wymienione poniżej pojęcia mają następujące znaczenia:

a) **Nadzór nad bezpieczeństwem** określa to, co Państwo wykonuje w stosunku do SMS operatorów/podmiotów lotniczych;

b) **Zapewnienie bezpieczeństwa** określa to, co Państwo wykonuje w odniesieniu do efektywności swojego SSP w zakresie bezpieczeństwa, a operatorzy/podmioty lotnicze wykonują w odniesieniu do efektywności swojego SMS w zakresie bezpieczeństwa, włącznie z monitorowaniem i analizą;

c) **Audyt bezpieczeństwa** jest czynnością wykonywaną przez Państwo w odniesieniu do struktury swojego SSP oraz wykonywaną przez operatorów/dostawców usług w odniesieniu do struktury swojego SMS.

*Uwaga.* – Audyt bezpieczeństwa jest czynnością wykonywaną przez ICAO i USOAP w odniesieniu do krajowego programu bezpieczeństwa władzy lotniczej i jej zdolności do prowadzenia nadzoru zgodnie z ICAO SARP i odpowiednimi materiałami pomocniczymi.

## 7.10 RÓŻNICE POMIĘDZY SLOGANAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM A ZASADAMI BEZPIECZEŃSTWA

7.10.1 Już od dawna w lotnictwie pojawia sie tendencja do polegania na sloganach dla pobudzenia świadomości o problemach związanych z bezpieczeństwem, tendencja, która często prowadzi do mylenia sloganów z zasadami. Pomiędzy sloganami a zasadami jest bardzo duża różnica. Zasady wyraźnie określają precyzyjne wytyczne oparte na rzetelnej wiedzy i zawierają pełne opisy jak realizować konkretne przedsięwzięcie. Slogany wyrażają niewyraźne aluzje oparte na tradycyjnej i często wątpliwej, powszechnie znanej wiedzy (wiedzy ludowej), i zazwyczaj błędnie obrazują sposób podejścia do zagadnienia. Podjęcie wysiłku w obszarze krytycznym, takim jak zarządzanie bezpieczeństwem i uruchomienie SSP/SMS w oparciu o głoszone slogany wykraczałoby poza zdrowy rozsądek. Jednak taka możliwość występuje. Niniejszy podrozdział omawia i stara się zdyskredytować pięć najbardziej popularnych sloganów dotyczących bezpieczeństwa, konfrontując je z koncepcjami dotyczącymi bezpieczeństwa i zarządzania bezpieczeństwem omówionymi w rozdziale 2:

a) W lotnictwie bezpieczeństwo jest na pierwszym miejscu.

b) Każdy odpowiada za bezpieczeństwo.

c) Jeżeli coś nie jest zepsute, to dlaczego to naprawiać?

d) Jeżeli uważasz, że bezpieczeństwo jest drogie, wypróbuj wypadek.

e) Siedemdziesiąt procent wypadków spowodowanych jest czynnikiem ludzkim.

7.10.2 **W lotnictwie bezpieczeństwo jest na pierwszym miejscu**. Organizacje umiejscowione w systemach produkcyjnych, zgodnie z nazwą, za swój cel stawiają zadania produkcyjne, takie jak produkcja samochodów, wydobywanie ropy lub jak w przypadku lotnictwa zarobkowego, transportowania drogą powietrzną ludzi i towarów. Organizacje umiejscowione w systemach produkcyjnych muszą zarabiać pieniądze dzięki swojej działalności, aby zagwarantować odpowiednie zasoby dla zrealizowania swoich celów produkcyjnych. W myśl tej zasady trudno byłoby więc zrozumieć jak bezpieczeństwo mogłoby być w lotnictwie na pierwszym miejscu, gdyż raczej należałoby domniemywać, że na pierwszym miejscu powinny się znaleźć pieniądze. Jak omówiono to w rozdziale 2 bezpieczeństwo w lotnictwie jest kwestią rozsądnej koordynacji priorytetów produkcyjnych i założeń

bezpieczeństwa, tak, aby organizacje lotnicze mogły w sposób bezpieczny zarabiać pieniądze. Pomieszanie priorytetów zawartych w tym sloganie często doprowadzało do niewłaściwych działań. I rzeczywiście, najczęstszym, po wykryciu niekorzystnych zdarzeń, argumentem wysuwanym przez niewłaściwie działające organizacje, niezależnie od dowodów potwierdzających przeciwną sytuację było to, że nie mogą zrozumieć, w jaki sposób doszło do tej niekorzystnej sytuacji, gdyż „w naszej firmie bezpieczeństwo stoi na pierwszym miejscu". Można to potwierdzić historycznymi zapisami, w myśl których organizacje, które kryły się za tym sloganem nie wspierając go odpowiednimi działaniami znalazły się wśród najgorszych pod względem łamania zasad bezpieczeństwa.

7.10.3 **Każdy odpowiada za bezpieczeństwo**. Ten slogan jest zagadką. Gdy ktoś czuje się źle, idzie do lekarza. Gdy potrzebne jest doradztwo prawne należy udać się do radcy prawnego. Jeżeli woda nie leje się z kranu trzeba wezwać hydraulika. Jednak, gdy trzeba stawić czoła problemom związanym z bezpieczeństwem, każdy w lotnictwie uważa się za eksperta w tej dziedzinie, szczególnie, jeżeli ma kilkuletnie doświadczenie w tym obszarze. Prawdą jednak jest fakt, że tylko wyszkoleni specjaliści mogą w sposób skuteczny wypowiadać się na temat problemów związanych z bezpieczeństwem. Najlepiej zarządzane organizacje lotnicze zatrudniają wyspecjalizowany personel ds. bezpieczeństwa, posiadający kwalifikacje zawodowe, dokładnie opisane stanowiska pracy, zdefiniowane obowiązki oraz dostęp do całej organizacji. Ci zawodowcy przyjmują na siebie odpowiedzialność „strażników" bezpieczeństwa w organizacji. Koordynują plany, aby ocenić i wzmocnić wewnętrzną odporność organizacji na potencjalne zagrożenia właściwe dla lotnictwa, których pozostali pracownicy muszą przestrzegać. Nie szukają usilnie winnych za nieodpowiednio zarządzane zagrożenia lub problemy związane z bezpieczeństwem, a raczej pracują nad odpowiednią dokumentacją i opisem w celu wypracowania satysfakcjonujących rozwiązań. Rozdział 8 do pewnego stopnia omawia te zagadnienia.

7.10.4 **Jeżeli coś nie jest zepsute, to dlaczego to naprawiać?** Ten slogan sugeruje, że nie należy interesować się bezpieczeństwem, dopóki nie ma wypadków, że system jest bezpieczny dopóki nikomu nic się nie stanie, a organizacja nie będzie narażona na krytykę i przykre konsekwencje. Innymi słowy slogan zakłada, że wypadki lub ich BRAK są wiarygodnymi wskaźnikami systemu bezpieczeństwa. Alternatywny pogląd do powyższej myśli zakłada, że jeżeli struktury i procesy są na właściwym miejscu i system znajduje się pod ciągłym nadzorem oczekując na sygnały o zagrożeniach, to wypadki stanowią niefortunne „zakłócenia w systemie". Oprócz innych nieprawd kryjących się za tym sloganem, jak pokazano w rozdziale 3, czekanie z usunięciem niedociągnięć w zakresie bezpieczeństwa na załamanie systemu może okazać się nieracjonalnie uciążliwym. Ponadto, gdy następuje załamanie systemu, życie ludzkie jest zagrożone, a to, w odniesieniu do takiego podejścia, nasuwa pytania o charakterze etycznym. Ponieważ skutki finansowe i ludzki wysiłek związany z działaniami naprawczymi podjętymi dopiero po wypadku są niewspółmiernie wysokie, występują zatem nieodparte powody ekonomiczne i etyczne, aby naprawić system zanim się zepsuje.

7.10.5 **Jeżeli uważasz, że bezpieczeństwo jest drogie, wypróbuj wypadek.** Powszechne przekonanie ukryte pod tym sloganem to stwierdzenie, że obserwując postawę zawodową, nakładając dyscyplinę i przestrzegając profesjonalnych standardów postępowania można przewidzieć wszystkie wady w systemie, które w jakimś momencie mogą doprowadzić do wypadku. Krótko mówiąc, zgodność prawna i „praca zgodnie z przepisami" stanowią wystarczającą gwarancję bezpieczeństwa. Niestety, jak pokazuje praktyka omówiona w rozdziale 3, w rzeczywistości mamy do czynienia z odmiennym scenariuszem. Jeżeli wszystkie struktury i procesy są na miejscu, wypadki takie jak choroba czy śmierć stają sie wyłącznie przypadkiem statystycznym. Podczas gdy jest możliwym i sensownym angażowanie się i prowadzenie wyprzedzających czynności takich jak sprawdzanie działania systemu, podobnie jak to czynią ludzie chodząc do lekarza rodzinnego i angażując się w programy zdrowotne, jest absolutnie niemożliwym wyeliminowanie wszystkich zagrożeń. Zagrożenia są integralnymi elementami kontekstu operacyjnego lotnictwa. Awaria i błędy operacyjne będą się zdarzać w lotnictwie, pomimo najlepszych i prawie całkowicie zrealizowanych wysiłków w celu ich uniknięcia. W skutecznej organizacji zatrudniającej wykwalifikowanych pracowników oraz posiadającej odpowiednie zasoby dla realizowania swoich założeń produkcyjnych i mającej dobrze opracowane procedury zawsze może zdarzyć się wypadek, podczas gdy w źle zarządzanej, niedofinansowanej organizacji zatrudniającej pracowników o wątpliwych kwalifikacjach, stosującej praktyki poniżej standardu, i posiadającej historię „było blisko" można uniknąć wypadku przez zwykłe szczęście.

7.10.6 **Siedemdziesiąt procent wypadków spowodowanych jest czynnikiem ludzkim.** Ten slogan został zachowany na koniec, gdyż podkreśla jak mylące mogą być slogany dotyczące bezpieczeństwa. Rozważmy system lotnictwa: ludzie starają się zrozumieć plan systemu i gdy już uważają, że wszystko zrozumieli, przystępują do jego projektowania. Następnie system konstruują i kiedy już nadaje się do użytku uruchamiają go. W celu wykazania, że system zachowuje się w sposób umożliwiający spełnienie jego założeń, ludzie szkolą innych ludzi, którzy ten system każdego dnia uruchamiają. Ludzie podejmują strategiczne i taktyczne decyzje związane z działaniem systemu, a kiedy zidentyfikowane są zagrożenia, wymyślają i uruchamiają działania, aby uchronić system przed tymi zagrożeniami. Krótko mówiąc: ludzie projektują, produkują, szkolą, obsługują, zarządzają i bronią systemu. Tak więc, gdy system załamie się, siłą rzeczy przyczyną jest ludzki błąd. Z tej perspektywy i w zależności od poziomu obserwacji dowiedziono, że sto procent wypadków spowodowanych jest przez czynnik ludzki.

## Dodatek 1 do Rozdziału 7

# OPIS SYSTEMU – WYTYCZNE

### 1. WPROWADZENIE

1.1 Sporządzenie opisu systemu jest podstawowym warunkiem stworzenia w organizacji systemu zarządzania bezpieczeństwem (SMS). Każdy system posiada potencjalnie słabe punkty w obszarze bezpieczeństwa, które są identyfikowane w warunkach zagrożenia. W procesie identyfikacji zagrożeń istnieje możliwość identyfikacji tylko tych, które wchodzą w zakres opisu systemu. W związku z takim formalnym podejściem, opisywany obszar powinien być na tyle szeroko zakreślony, aby obejmował wszystkie możliwe zagrożenia, z którymi system potencjalnie mógłby się zmierzyć lub wygenerować. Szczególnie ważne jest, aby opis zawierał powiązania wewnątrz systemowe, jak również powiązania z większymi systemami, których ten system jest częścią.

1.2 Szczegółowy opis systemu powinien zawierać:

a) cel systemu;

b) sposób wykorzystania systemu;

c) funkcje systemu;

d) obszar działania systemu i zewnętrzne powiązania;

e) otoczenie, w którym system będzie funkcjonował.

1.3 Konsekwencje dla bezpieczeństwa z powodu potencjalnej utraty albo obniżenia wydajności systemu mogą być częściowo determinowane poprzez właściwości otoczenia operacyjnego, z którym system będzie integrowany. Dlatego też, opis otoczenia powinien uwzględniać wszystkie czynniki, które mogłyby mieć znaczący wpływ na bezpieczeństwo. Czynniki te mogą się różnić w zależności od organizacji. Opis może na przykład uwzględniać zarówno cechy właściwe dla ruchu powietrznego, jak i naziemnego, infrastrukturę lotniska i czynniki pogodowe. Opis systemu powinien też wskazywać na inne, wariantowe procedury i zdarzenia odbiegające od normy, na przykład awaria łączności lub urządzeń nawigacji. Poniżej przykładowy opis systemu lotniskowego.

### 2. OPIS SYSTEMU LOTNISKOWEGO

Opis systemu lotniskowego powinien zawierać informacje na temat urządzeń, sprzętu, personelu, procesów i procedur koniecznych dla funkcjonowania lotniska.

Zróżnicowane działania mogą uwzględniać:

1. Zarządzanie operacyjne.

    1.1 Kontrola dostępu do obszaru ruchu:

        a) Powietrze

        b) Ziemia

        c) Morze

    1.2 Planowanie działania w sytuacji kryzysowej na lotnisku:

        a) Podręcznik procedur postępowania w sytuacjach kryzysowych

        b) Praktyczne modele postępowania w sytuacjach kryzysowych

1.3 Służby ratownicze i straż pożarna:

a) Zdolność operacyjna

1) Sprzęt
2) Poziom sprawności gaśnic pianowych/ wodnych / proszkowych

b) Konserwacja i utrzymanie sprzętu

c) Poziom wyszkolenia i doświadczenia personelu

d) Plan mobilizacji sprzętu

e) Ograniczenia zdatności (uwagi)

f) System hydrantów wodnych

1.4 Kontrola i utrzymanie obszaru ruchu:

a) Podręcznik procedur lotniskowych

b) Formularze kontrolne

c) Utrzymanie

1.5 Wizualna pomoc w utrzymaniu gotowości:

a) Inspekcje

b) Harmonogramy

1.6 Zarządzanie robotami budowlanymi:

a) Kontrola robót

b) Zarządzanie placem budowy

1.7 Zarządzanie bezpieczeństwem na płycie postojowej lotniska, włączając ruch pojazdów:

a) Zasady i przepisy dotyczące operacji na płycie lotniska

b) Zarządzanie płytą lotniska

1) Zarządzanie pojazdami na płycie lotniska
2) Pozwolenia dla pojazdów poruszających się po płycie lotniska
3) Badania techniczne pojazdów
4) Instrukcja bezpieczeństwa
5) Koordynacja obsługi statków powietrznych

c) Sprzęt do parkowania

d) Dyscyplina na płycie postojowej lotniska

e) Operacja wypychania (*push-back)* statków powietrznych

f ) Oznakowanie pionowe i poziome

g) Alokacja stanowisk postojowych

h) Kontrola uszkodzeń statku powietrznego

i) Kontrole wycieku paliwa

j) Kontrola uszkodzeń pojazdów i sprzętu

k) Wykaz elementów sprawdzających poziom bezpieczeństwa na płycie postojowej, w tym audyt na rampie

l) Działalność własna i zlecana podwykonawcom

1.8 Zagrożenia związane z dzikimi zwierzętami:

a) Kontrola zagrożenia ze strony ptaków

b) Obserwacja ptaków

c) Zarządzanie raportami ze zderzeń ptaków ze statkami powietrznymi

1.9 Kontrola pod kątem obecności obiektów obcych:

a) W granicach portu lotniczego

b) Poza granicami portu lotniczego

c) Na pasie startowym

d) Przepisy i inspekcje

e) Zatwierdzanie zezwoleń na budowę konstrukcji i budynków na ścieżce podejścia do lądowania

1.10 Usuwanie niesprawnego statku powietrznego:

a) Sprzęt kompatybilny z typem statku powietrznego

b) Utrzymywanie w gotowości

c) Plan rozlokowania

d) Stworzenie procedur dla dostawców zewnętrznych/ustalenie kontaktów

1.11 Obsługa towarów niebezpiecznych:

a) Ograniczenia przewozu niebezpiecznych towarów na pokładzie statku powietrznego

b) Przechowywanie i załadunek

c) Stworzenie programu szkoleń

d) Akceptacja niebezpiecznych towarów przez operatora

e) Wytyczne jak reagować na zagrożenie powstałe w wyniku zdarzenia lotniczego z udziałem towarów niebezpiecznych

1.12 Ograniczona widzialność i niekorzystne warunki pogodowe wykonywania operacji:

a) Procedury

b) Koordynacja działań ze służbami kontroli ruchu lotniczego

c) Odpowiedzialność podmiotów włączonych w działania

1.13 Instalacja i utrzymanie radiowych pomocy nawigacyjnych:

a) NOTAMS

2. Zarządzanie lotniskiem.

2.1 Negocjacje slotów i ich alokacja

2.2 Odprawianie rejsów

2.3 Wytyczne dla służb asystujących przy kołowaniu statku powietrznego i zabezpieczaniu do postoju na płycie

2.4 Zarządzanie płytą postojową i alokacja stanowisk postojowych

2.5 Operacje o ograniczonej widzialności CAT II i CAT III

2.6 Zasady kontroli ruchu i licencjonowanie operacji

2.7 Sprzątanie, usuwanie/śmieci i ochrona przed szkodnikami i insektami

3. Zarządzanie budynkiem Terminala pasażerskiego.

   3.1 Zarządzanie ruchem pasażerów, przepływem bagaży i wyposażeniem Terminala.

   3.2 Informacja ogólna dla pasażerów

   3.3 Obsługa pasażerów VIP i CIP

   3.4 Bagaże pozostawione bez opieki

   3.5 Asysta bagażowych

   3.6 Zarządzanie wózkami bagażowymi

   3.7 Sprzątanie i ochrona przed szkodnikami i insektami

4. Informacja lotniskowa i dotycząca ruchu powietrznego oraz usługi komunikacyjne.

   4.1 Kontrola ruchu lotniczego (lotniskowy nadzór nad operacjami w sytuacji ograniczonej widzialności)

   4.2 Służby powiadamiania i informacyjne na temat rejsów.

   4.3 Lotniskowe służby (biuro dla służb opracowujących notamy i informacje przedstartowe)

   4.4 Lotniskowe służby telekomunikacyjne

5. Zarządzanie ochroną i bezpieczeństwem.

   5.1 Wdrożenie i monitorowanie systemu zarządzania bezpieczeństwem SMS

      a) Zarządzający systemem bezpieczeństwa

      b) Identyfikacja zagrożeń i ocena konsekwencji

      c) Ocena ryzyka, kontrola i łagodzenie skutków

      d) Zapewnienie bezpieczeństwa

      e) Zespoły operacyjne ds. bezpieczeństwa

      f) Podręcznik Systemu Zarządzania Bezpieczeństwem (SMSM)

   5.2 Implementacja i monitorowanie programu bezpieczeństwa

   5.3 Implementacja i monitorowanie planu postępowania w sytuacji kryzysowej dla lotniska (AEP)

   5.4 Procedura przyjmowania wniosków na wydanie przepustek dostępu.

## Dodatek 2 do Rozdziału 7

# Wytyczne odnośnie rozwoju SMS
# Analiza luk w systemie bezpieczeństwa dostawców usług

*Uwaga. – W kontekście tego załącznika termin "dostawca usług" (service provider) odnosi się do każdej organizacji dostarczającej usługi dla lotnictwa. Termin ten obejmuje autoryzowane organizacje szkoleniowe, które są wystawione na ryzyko podczas świadczenia usług, operatorzy lotniczy, autoryzowane organizacje świadczące usługi w zakresie obsługi technicznej, konstruktorzy i producenci statków powietrznych, obsługa ruchu lotniczego i certyfikowane porty lotnicze, jeśli to ma zastosowanie.*

### 1. ANALIZA LUK

1.1 Wdrożenie Systemu Zarządzania Bezpieczeństwem (SMS) wymaga od dostawcy usług przeprowadzenia analizy systemu, aby określić, które składowe i elementy SMS są w danym momencie właściwe, a które muszą być dodane lub zmodyfikowane, tak, aby spełnione zostały kryteria niezbędne do wdrożenia systemu. Analiza ta jest znana jako analiza luk i obejmuje porównanie wymogów SMS do aktualnych możliwości ich realizacji przez dostawcę usług.

1.2 Analiza luk dostarcza, w formie listy kontrolnej, informacji mającej pomóc w ocenie, które ze składowych i elementów, odpowiadają strukturze SMS ICAO oraz zidentyfikować komponenty i elementy, które należy rozwinąć. W sytuacji, jeśli taka analiza zostanie zakończona i udokumentowana, stworzy ona podstawę do wypracowania spójnego planu implementacji SMS.

### 2. STRUKTURA SMS WEDŁUG ICAO

Struktura SMS zgodnie z wytycznymi ICAO składa się z czterech komponentów i dwunastu elementów, a jej implementacja będzie współmierna do wielkości organizacji i złożoności dostarczonych usług.

1. Polityka bezpieczeństwa i jej cele
   - 1.1 Zaangażowanie i odpowiedzialność Zarządu
   - 1.2 Odpowiedzialność w zakresie bezpieczeństwa
   - 1.3 Wyznaczenie personelu kluczowego dla systemu bezpieczeństwa
   - 1.4 Koordynacja planów reakcji w sytuacji kryzysowej
   - 1.5 Dokumentacja SMS
2. Zarządzanie ryzykiem
   - 2.1 Identyfikacja zagrożeń
   - 2.2 Ocena i łagodzenie ryzyka
3. Zapewnienie bezpieczeństwa
   - 3.1 Monitorowania realizacji założeń bezpieczeństwa i analiza
   - 3.2 Zarządzanie zmianami
   - 3.3 Kontynuacja usprawniania SMS
4. Promocja bezpieczeństwa
   - 4.1 Szkolenie i kształcenie
   - 4.2 Komunikacja w zakresie bezpieczeństwa

### 3. ANALIZA LUK W SYSTEMIE ZARZĄDZANIA BEZPIECZEŃSTWEM (SMS) DLA PODMIOTÓW ŚWIADCZĄCYCH USŁUGI LOTNICZE

Zamieszczona poniżej lista kontrolna może być wykorzystana jako wzór do przeprowadzania analizy luk. Każde pytanie jest sformułowane w taki sposób, aby uzyskać odpowiedź „TAK" lub „NIE". Odpowiedź "Tak" wskazuje, że podmiot świadczący usługi posiada już w swoim systemie komponent albo element struktury systemu zarządzania bezpieczeństwem zgodnie z wytycznymi ICAO i w tym przypadku wypełnia lub przewyższa oczekiwane wymagania. Odpowiedź „NIE" wskazuje, że istnieje luka pomiędzy komponentem/elementem struktury systemu zarządzania bezpieczeństwem ICAO i systemu podmiotu świadczącego usługi lotnicze.

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Komponent 1 — POLITYKA BEZPIECZEŃSTWA I JEJ CELE** | | | |
| **Element 1.1 — Zaangażowanie i odpowiedzialność Zarządu** | | | |
| Rozdział 8 | Czy w organizacji wdrożona jest polityka bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 3 i 8 | Czy polityka bezpieczeństwa odzwierciedla zaangażowanie organizacji w zakresie zarządzania bezpieczeństwem? | □ Tak<br>□ Nie | |
| Rozdział 3 i 8 | Czy w ramach polityki bezpieczeństwa zostało sformułowane jasne przesłanie odnośnie konieczności zapewnienia niezbędnych środków na jej wdrażanie? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy polityka bezpieczeństwa obejmuje procedury raportowania na temat bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy polityka bezpieczeństwa wyraźnie wskazuje, jakie rodzaje działań operacyjnych są nieakceptowalne? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy polityka bezpieczeństwa uwzględnia warunki na podstawie, których działania dyscyplinujące nie miałyby zastosowania? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy polityka bezpieczeństwa jest zatwierdzona i podpisana przez zarząd organizacji? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy informacje na temat polityki bezpieczeństwa są przekazywane pracownikom przy wyraźnym wsparciu ze strony zarządu? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy polityka bezpieczeństwa jest okresowo przeglądana w celu upewnienia się, czy nadal jest odpowiednia dla organizacji? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy istnieje formalny program rozwoju spójnego planu realizacji celów bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy cele dotyczące bezpieczeństwa mają powiązanie ze wskaźnikami wykonania, celami i planem działania w zakresie bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy informacje dotyczące polityki bezpieczeństwa są publikowane i dystrybuowane? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Element 1.2 — Odpowiedzialność w zakresie bezpieczeństwa** | | | |
| Rozdział 8 i 10 | Czy [Organizacja] wyznaczyła osobę zarządzającą, która pomimo pełnienia innych funkcji, będzie ostatecznie odpowiedzialna, w imieniu [organizacji], za wprowadzanie i utrzymanie SMS? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba Zarządzająca jest odpowiedzialna za zapewnienie, że system zarządzania bezpieczeństwem jest właściwie wdrażany i spełnia wymagania we wszystkich obszarach [organizacji]? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba zarządzająca posiada pełne upoważnienia finansowe wymagane do prowadzenia certyfikowanej działalności operacyjnej? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba Zarządzająca posiada pełną kontrolę zasobów ludzkich wymaganych do prowadzenia certyfikowanej działalności operacyjnej? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba Zarządzająca ponosi bezpośrednią odpowiedzialność za prowadzenie spraw [organizacji]? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba zarządzająca posiada kompletne pełnomocnictwa do prowadzenia certyfikowanej działalności operacyjnej? | □ Tak<br>□ Nie | |
| Rozdział 8 i 10 | Czy w [organizacji] jest zdefiniowany zakres odpowiedzialności wszystkich członków zarządu jak również pracowników niezależnie od ich innych funkcji, odnośnie działań na rzecz bezpieczeństwa w ramach SMS? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy zakres obowiązków, odpowiedzialności oraz pełnomocnictw jest udokumentowany i rozpowszechniony w ramach [organizacji ]? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy [organizacja] dokładnie określa, które szczeble kadry zarządzającej mają pełnomocnictwa do podejmowania decyzji w zakresie stopnia akceptowania ryzyka? | □ Tak<br>□ Nie | |
| **Element 1.3 — Wyznaczenie personelu kluczowego dla systemu bezpieczeństwa** | | | |
| Rozdział 8 | Czy [organizacja] wyznaczyła wykwalifikowaną osobę do prowadzenia i codziennego monitorowania funkcjonowania SMS? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy osoba doglądająca funkcjonowania SMS wypełnia obowiązki i wymagania wynikające z zakresu czynności i odpowiedzialności? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy w [organizacji] istnieją zdefiniowane i udokumentowane pełnomocnictwa, zakresy obowiązków i odpowiedzialności dla personelu wszystkich szczebli? | □ Tak<br>□ Nie | |
| **Element 1.4 — Koordynacja planów reagowania w sytuacji kryzysowej** | | | |
| Rozdział 8 | Czy [organizacja] posiada adekwatny do swojej wielkości, natury i złożoności plan reakcji w sytuacji zagrożenia/plan awaryjny? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy [organizacja] koordynuje swoje procedury w zakresie reagowania/prowadzenia działań w sytuacji kryzysowej z procedurami innych organizacji, z którymi musi współdziałać podczas świadczenia usług? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy [organizacja] posiada instrukcje dotyczące sposobów dystrybucji i komunikowania procesu koordynacji procedur w odniesieniu do personelu zaangażowanego w takie współdziałanie? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Element 1.5 — Dokumentacja SMS** | | | |
| Rozdział 4 i 8 | Czy [Organizacja] stworzyła i utrzymuje archiwum zawierające odpowiednią dokumentację bezpieczeństwa i zarządzania ryzykiem? | □ Tak<br>□ Nie | |
| Rozdział 4 i 8 | Czy organizacja stworzyła I utrzymuje dokumentację dotycząca SMS w formie papierowej lub elektronicznej? | □ Tak<br>□ Nie | |
| Rozdział 7, 8 i 10 | Czy dokumentacja SMS jest stworzona w sposób opisujący SMS i skonsolidowane relacje pomiędzy wszystkimi jego komponentami ? | □ Tak<br>□ Nie | |
| Rozdział 8 i 10 | Czy podmiot lotniczy usługi opracował plan wdrożenia SMS, który zapewnia, że wszystkie cele organizacji w zakresie bezpieczeństwa są spełnione? | □ Tak<br>□ Nie | |
| Rozdział 8 i 10 | Czy plan wdrożenia SMS został stworzony przez osoby albo grupy posiadające odpowiednie doświadczenie? | □ Tak<br>□ Nie | |
| Rozdział 8 i 10 | Czy osoba lub grupa osób miała wystarczający dostęp do zasobów (w tym czas na spotkania), aby stworzyć plan wdrożenia SMS? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy plan wdrożenia SMS został zaakceptowany przez wyższy szczebel kierowniczy organizacji? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy plan wdrożenia SMS jest regularnie przeglądany przez wyższy szczebel kierowniczy organizacji? | □ Tak<br>□ Nie | |
| Rozdział 8 i 10 | Czy plan wdrożenia SMS przewiduje możliwość implementacji systemu etapami? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy plan wdrożenia SMS jednoznacznie określa zasady koordynacji pomiędzy SMS dostawcy usługi i SMS innych podmiotów, z którymi organizacja musi być skorelowana w trakcie świadczenia usług? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy podmiot lotniczy usługi stworzył podręcznik SMS jako podstawowy instrument komunikowania ich podejścia do zasad bezpieczeństwa w całej [organizacji]? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy podręcznik SMS dokumentuje wszystkie aspekty SMS włączając miedzy innymi politykę bezpieczeństwa, cele, procedury i indywidualną odpowiedzialność za bezpieczeństwo? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy podręcznik SMS wyraźnie określa rolę zarządzania ryzykiem jako początkowej działalności projektowej i rolę zapewnienia bezpieczeństwa jako działalności ciągłej? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy odpowiednie części dokumentacji powiązanej z SMS są włączone w istniejącą, zaakceptowaną w organizacji dokumentację taką jak podręcznik operacyjny firmy, nadzór nad utrzymaniem/ podręcznik regulujący politykę firmy/ instrukcja operacyjna służb lotniskowych, jeśli mają zastosowanie? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy podmiot lotniczy usług posiada system rejestracji, który gwarantuje tworzenie i przechowywanie wszystkich zapisów koniecznych, by dokumentować i wspomagać wymagania operacyjne? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy system rejestrujący dostawcy usług jest zgodny z odpowiednimi wymaganiami objętymi regulacją i dobrą praktyką w ramach branży? | □ Tak<br>□ Nie | |
| Rozdział 8 | Czy system rejestracji danych przewiduje nadzór nad procesami, konieczny do zapewnienia odpowiedniej identyfikacji, czytelności, sposobu przechowywania, ochrony, archiwizowania, odzyskiwania, czasu przechowywania i rozporządzania zapisami? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Komponent 2 — Zarządzanie ryzykiem bezpieczeństwa** | | | |
| **Element 2.1 — Identyfikacja zagrożeń** | | | |
| Rozdział 3 i 9 | Czy organizacja posiada formalny system gromadzenia informacji odnośnie bezpieczeństwa i system przetwarzający w sposób efektywny dane odnośnie zagrożeń w prowadzeniu operacji (SDCPS)? | □ Tak<br>□ Nie | |
| Rozdział 3, 4 i 9 | Czy SDCPS [organizacji] zakłada przy gromadzeniu informacji na temat zagrożeń bezpieczeństwa stosowanie kombinacji metod reaktywnej, proaktywnej i prognostycznej? | □ Tak<br>□ Nie | |
| Rozdział 3, 9 i 10 | Czy [organizacja] stosuje reaktywne metody w procesie prowadzącym do zgromadzenia odpowiednich danych na temat bezpieczeństwa i zarządzania ryzykiem? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy podmiot lotniczy usług wprowadził szkolenia na temat reaktywnych metod gromadzenia danych dotyczących bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy podmiot lotniczy usług wprowadził zasady komunikacji w związku z reaktywnymi metodami gromadzenia danych dotyczących bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy metoda reaktywnego raportowania jest prosta, dostępna i współmierna z wielkością dostawcy usług? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy raporty sporządzane na podstawie identyfikacji zdarzeń przy pomocy metody reaktywnej są przeglądane przez właściwy szczebel kierowniczy? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura powiadamiania współpracowników o otrzymaniu ich raportów wraz z procesem dzielenia się rezultatami przeprowadzonej analizy? | □ Tak<br>□ Nie | |
| Rozdział 3, 9 i 10 | Czy podmiot lotniczy usług stosuje proaktywne procedury umożliwiające czynną identyfikację ryzyk w zakresie bezpieczeństwa poprzez analizę działalności organizacji? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy szkolenia obejmują proaktywne metody gromadzenia danych na temat bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy podmiot lotniczy usług wprowadził zasady komunikacji w związku z proaktywnymi metodami gromadzenia danych dotyczących bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy metoda proaktywnego raportowania jest prosta, dostępna i współmierna z wielkością dostawcy usług? | □ Tak<br>□ Nie | |
| Rozdział 3, 9 i 10 | Czy podmiot lotniczy usług stosuje zapobiegawczo procedury, które zapewniają zapis działalności systemu w czasie rzeczywistym wykonywania normalnych operacji? | □ Tak<br>□ Nie | |
| Rozdział 9 i 10 | Czy szkolenia obejmują prognostyczne metody gromadzenia danych na temat bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy podmiot lotniczy usług wprowadził zasady komunikacji w związku z prognostycznymi metodami gromadzenia danych dotyczących bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy procedury zapisywania prognostycznych danych dotyczących bezpieczeństwa są współmierne do wielkości dostawcy usługi? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Element 2.2 — Ocena i łagodzenie ryzyka bezpieczeństwa** | | | |
| Rozdział 9 i 10 | Czy [Organizacja] wprowadziła i utrzymuje sformalizowane procesy zapewniające analizę, oszacowanie i kontrolę ryzyka w zakresie bezpieczeństwa w operacjach [organizacji]? | □ Tak<br>□ Nie | |
| Rozdział 4, 9 i 10 | Czy dokumentacja SMS [organizacji] jasno definiuje powiązania pomiędzy zagrożeniami, konsekwencjami i ryzykiem w zakresie bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 5 i 9 | Czy istnieją ustrukturyzowane procesy dla prowadzenia analiz ryzyka powstałego w następstwie zidentyfikowanych zagrożeń, wyrażonych w warunkach prawdopodobieństwa i powagi zdarzenia? | □ Tak<br>□ Nie | |
| Rozdział 5 i 9 | Czy istnieją kryteria szacowania i ustalania akceptowalności ryzyka {np. poziom ryzyka, który organizacja jest skłonna zaakceptować}? | □ Tak<br>□ Nie | |
| Rozdział 5 i 9 | Czy podmiot lotniczy usług stosuje strategię łagodzenia ryzyka, zawierającą mechanizmy naprawcze/prewencyjne, aby zapobiegać powtarzaniu się odnotowanych nieprawidłowości? | □ Tak<br>□ Nie | |
| **Komponent 3 — Zapewnienie bezpieczeństwa** | | | |
| **Element 3.1 — Monitorowania realizacji założeń bezpieczeństwa i ich analiza** | | | |
| Rozdział 9 i 10 | Czy [Organizacja] wdrożyła wewnętrzne procesy mające na celu weryfikację poziomu realizacji założeń bezpieczeństwa w [organizacji] oraz sprawdzanie efektywności kontroli ryzyka? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy w powyższych procesach wykorzystywane są następujące narzędzia?<br>"System raportowania bezpieczeństwa" Tak / Nie<br>"Analiza bezpieczeństwa" Tak / Nie<br>"Przeglądy bezpieczeństwa" Tak / Nie<br>"Audyty bezpieczeństwa" Tak / Nie<br>"Inspekcje bezpieczeństwa" Tak / Nie<br>"Wewnętrzne badania poziomu bezpieczeństwa" Tak / Nie | | |
| Rozdział 6 i 9 | Czy kontrola realizacji bezpieczeństwa w [organizacji] odbywa się w odniesieniu do wskaźników bezpieczeństwa oraz wypełniania celów SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy raporty dotyczące bezpieczeństwa są przeglądane przez odpowiednie szczeble kadry zarządzającej? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy funkcjonuje system informacji zwrotnej, mający na celu powiadomienie współpracowników o otrzymaniu przekazanych raportów i dzielenia się rezultatami analizy tych materiałów? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy działania naprawcze i prewencyjne są opracowywane w odpowiedzi na identyfikację zagrożeń? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieją wdrożone procedury prowadzenia wewnętrznych dochodzeń? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieją procedury zapewniające, że zgłoszone zdarzenia i nieprawidłowości są analizowane pod kątem identyfikacji wszystkich współistniejących zagrożeń? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| Rozdział 9 | Czy usługodawca posiada procedury oceny efektywności pomiarów wdrożonych działań naprawczych/prewencyjnych? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy usługodawca posiada system monitorowania wewnętrznych procesów raportowania i podejmowanych w związku z nim działań naprawczych? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy system audytów pokrywa wszystkie funkcje, działalność i struktury usługodawcy? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieją procedury selekcji/szkoleń zapewnienia obiektywności i kompetencji audytorów jak również bezstronności procesu prowadzenia audytu? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura raportowania wyników audytu i przechowywania zapisów pokontrolnych? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura określająca wymagania odnośnie terminowego podjęcia działań korygujących w odpowiedzi na wyniki audytu? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura umożliwiająca rejestrowanie sposobów weryfikacji podejmowanych działań i raportowania efektów weryfikacji tych działań? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje wdrożony proces monitorowania i analizowania trendów? | □ Tak<br>□ Nie | |
| **Element 3.2 — Zarządzanie zmianami** | | | |
| Rozdział 9 | Czy [Organizacja] wdrożyła i utrzymuje formalne procesy identyfikacji zmian w organizacji, które mogłyby oddziaływać na obowiązujące procesy i usługi? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy formalny proces zarządzania zmianami analizuje zmiany działania lub zmiany personelu kluczowego dla zagrożeń bezpieczeństwa? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy [organizacja] podjęła działania w celu zapewnienia poziomu bezpieczeństwa przed wdrożeniem zmian? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy [organizacja] uruchomiła proces eliminowania albo zmian kontroli ryzyka bezpieczeństwa, które nie są już potrzebne z powodu zmian w środowisku operacyjnym? | □ Tak<br>□ Nie | |
| **Element 3.3 — Kontynuacja usprawniania SMS** | | | |
| Rozdział 9 | Czy [organizacja] rozwinęła i utrzymuje sformalizowany proces identyfikacji przyczyn działania SMS poniżej standardu? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy [organizacja] stworzyła mechanizm(y) ustalania skutków działania SMS operacji poniżej określonego standardu? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy [organizacja] stworzyła mechanizm(y) eliminowania lub ograniczenie przyczyn niskiego standardu wykonywania SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy [organizacja] stosuje procesy proaktywnej oceny sprzętu, wyposażenia, dokumentacji i procedur (poprzez audyty, ankiety, itd)? | □ Tak<br>□ Nie | |

| Odniesienie ICAO | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| Rozdział 9 | Czy organizacja stosuje proces proaktywnej oceny skuteczności poszczególnych osób, w celu sprawdzenia poziomu wypełniania swoich obowiązków w zakresie bezpieczeństwa? | □ Tak<br>□ Nie | |
| **Komponent 4 — Promowanie bezpieczeństwa** | | | |
| **Element 4.1 — Szkolenie i edukacja** | | | |
| Rozdział 9 | Czy istnieje udokumentowany proces identyfikacji wymogów szkoleniowych, aby personel był wytrenowany i kompetentny w wykonywaniu swoich obowiązków w zakresie SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy szkolenie w zakresie bezpieczeństwa jest dostosowane do stopnia zaangażowania danej osoby w SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy szkolenie w zakresie bezpieczeństwa jest włączone do szkolenia wstępnego dla zatrudnianych pracowników? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje program szkolenia w zakresie reagowania w sytuacji kryzysowej dla personelu dotkniętego taką sytuacją? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura mierząca skuteczność szkoleń? | □ Tak<br>□ Nie | |
| **Element 4.2 — Komunikacja w zakresie bezpieczeństwa** | | | |
| Rozdział 9 | Czy procesy komunikacyjne istniejące w organizacji umożliwiają efektywne funkcjonowanie SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy procesy komunikacyjne (pisemne, spotkania, elektroniczne, itd.) są współmierne do wielkości i zakresu działania usługodawcy? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy ważne informacje z zakresu bezpieczeństwa są przyjmowane i przechowywana na odpowiednim nośniku, zawierają wskazówki odnośnie dokumentów związanych z SMS? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy informacje krytyczne z zakresu bezpieczeństwa są rozpowszechniane w ramach [organizacji] i czy ich skuteczność jest monitorowana? | □ Tak<br>□ Nie | |
| Rozdział 9 | Czy istnieje procedura, która wyjaśnia, dlaczego podejmuje się konkretne działania dotyczące bezpieczeństwa i dlaczego procedury bezpieczeństwa są wprowadzone albo zmienione? | □ Tak<br>□ Nie | |

# Rozdział 8

# PLANOWANIE SMS

## 8.1 CEL I ZAWARTOŚĆ

Rozdział ten opisuje wymagania związane z planowaniem systemu zarządzania bezpieczeństwem, włączając również strukturę planu wdrażania SMS. Wymagania te opisane są w odniesieniu do ramowej struktury systemu zarządzania bezpieczeństwem Organizacji Międzynarodowego Lotnictwa Cywilnego ICAO. Chociaż struktura SMS ICAO jest wprowadzona jako całość, ten rozdział omawia wyłącznie pierwszy komponent, część składową struktury, jakim jest Polityka Bezpieczeństwa i jej cele. Pozostałe trzy komponenty struktury ramowej SMS ICAO (zarządzanie ryzykiem, zapewnienie bezpieczeństwa i promowanie bezpieczeństwa) są omawiane w Rozdziale 9. Ten rozdział zawiera następujące tematy :

a) Komponenty i elementy SMS;

b) Struktura SMS ICAO;

c) Zaangażowanie i odpowiedzialność Zarządu;

d) Zobowiązania w zakresie bezpieczeństwa;

e) Wyznaczenie personelu kluczowego dla systemu bezpieczeństwa;

f) Koordynacja planów reakcji w sytuacjach kryzysowych;

g) Dokumentacja SMS;

h) Plan implementacji SMS.

## 8.2 ELEMENTY I KOMPONENTY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM

8.2.1 Istnieją cztery elementy składowe SMS, które opisują dwa zasadnicze procesy, stanowiące jego podstawę, jak również ustalenia organizacyjne, niezbędne do wsparcia tych dwóch procesów operacyjnych. Tymi elementami SMS są :

a) polityka bezpieczeństwa i jej cele;

b) zarządzanie ryzykiem;

c) zapewnienie bezpieczeństwa;

d) promowanie bezpieczeństwa.

8.2.2 Dwa podstawowe obszary działalności operacyjnej w ramach SMS to: zarządzanie ryzykiem i zapewnienie bezpieczeństwa. Zarządzanie ryzykiem musi być rozpatrywane we wczesnym stadium projektowania systemu, mając na uwadze wstępną identyfikację zagrożeń w kontekście których będą się odbywały operacje związane z dostawą usług. Zapewnienie bezpieczeństwa należy uznać za stałe, bieżące działania mające na celu:

a) zapewnienie wstępnego rozpoznania zagrożeń i założenie w odniesieniu do oceny skutków ryzyka i zabezpieczeń istniejących w systemie jako środki kontroli, że pozostaną ważne i możliwe do zastosowania nawet, gdy system zmieni się w czasie i/albo

b) wprowadzenie koniecznych zmian w systemach zabezpieczających.

W tej sytuacji, identyfikacja zagrożenia może być rozpatrywana jako działania „one-stop" albo „one-shot", prowadzone w trakcie projektowania systemu albo w sytuacji, gdy do oryginalnego systemu muszą być wprowadzane znaczące zmiany. Z drugiej strony, zapewnienie bezpieczeństwa jest działalnością bieżącą, prowadzoną w sposób ciągły, w celu zapewnienia, że działania, które wspierają świadczenie usług, są należycie chronione przed zagrożeniami. Mówiąc najprościej, identyfikacja zagrożeń dostarcza wstępnych ram odniesienia dla procesu zapewnienia bezpieczeństwa, który musi być prowadzony codziennie.

8.2.3 Zasadnicze działania operacyjne prowadzone są pod auspicjami polityki bezpieczeństwa i jej celów, a wspomagane są poprzez promowanie bezpieczeństwa. Oba komponenty SMS obejmują niezbędne ustalenia organizacyjne, bez których identyfikacja zagrożenia i zarządzanie ryzykiem byłyby niemożliwe albo poważnie zakłócone. Dlatego też, oba komponenty, zarządzanie ryzykiem i zapewnienie bezpieczeństwa, w rzeczywistości tworzą SMS. Są to zatem komponenty działań operacyjnych, które tworzą podstawę funkcjonowania SMS. Z drugiej strony, polityka bezpieczeństwa, jej cele i promocja, dostarczają ram odniesienia oraz wsparcia, umożliwiając działalność operacyjną, podlegającą procesom zarządzania ryzykiem i zapewnienia bezpieczeństwa.

8.2.4 Cztery elementy omówione powyżej stanowią podstawowe składowe SMS, reprezentując cztery nadrzędne procesy zarządzania bezpieczeństwem, które leżą u podstaw rzeczywistego systemu zarządzania SMS. Każdy komponent jest podzielony na elementy, które obejmują szczegółowe podprocesy, konkretne zadania lub narzędzia, które, jak w zasadniczym systemie zarządzania, muszą być zaangażowane lub wykorzystane w celu zarządzania bezpieczeństwem, tak jak w każdej innej podstawowej działalności biznesowej lub procesach organizacyjnych.

8.2.5 Polityka bezpieczeństwa i jej cele składają się z pięciu elementów:

a) zaangażowanie i odpowiedzialność Zarządu;

b) zobowiązania w zakresie bezpieczeństwa;

c) wyznaczenie personelu kluczowego dla systemu bezpieczeństwa;

d) koordynacja planów reakcji w sytuacjach kryzysowych;

e) dokumentacja SMS.

8.2.6 Komponent - Zarządzanie ryzykiem składa się z dwóch elementów:

a ) identyfikacja zagrożeń;

b) ocena i łagodzenie ryzyka.

8.2.7 Komponent - Zapewnienie bezpieczeństwa składa się z trzech elementów:

a) monitorowanie realizacji założeń bezpieczeństwa i ich analiza (pomiar);

b) zarządzanie zmianami;

c) ciągła kontynuacja usprawniania SMS.

8.2.8 Komponent promowania bezpieczeństwa składa się z dwóch elementów:

a) szkolenie i edukacja;

b) komunikacja w zakresie bezpieczeństwa.

### 8.3 STRUKTURA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM ICAO

*Uwaga - Szczegóły struktury SMS ICAO są zawarte w Dodatku 1 do tego rozdziału.*

Cztery komponenty, połączone z dwunastoma elementami cząstkowymi omawianymi w sekcji 8.2, składają się na program ramowy SMS ICAO, zaplanowany jako zbiór zasad dla rozwoju i wdrożenia SMS przez dostawców usług, jak przedstawiono poniżej:

1. Polityka bezpieczeństwa i jej cele
   - 1.1 Zaangażowanie i odpowiedzialność Zarządu;
   - 1.2 Zobowiązania w zakresie bezpieczeństwa;
   - 1.3 Wyznaczenie personelu kluczowego dla systemu bezpieczeństwa;
   - 1.4 Koordynacja planów reakcji w sytuacjach kryzysowych;
   - 1.5 Dokumentacja SMS.
2. Zarządzanie ryzykiem
   - 2.1 Identyfikacja zagrożeń;
   - 2.2 Ocena i łagodzenie ryzyka.
3. Zapewnienie bezpieczeństwa
   - 3.1 Monitorowanie realizacji założeń bezpieczeństwa i ich analiza (pomiar);
   - 3.2 Zarządzanie zmianami;
   - 3.3 Kontynuacja usprawniania SMS.
4. Promowanie bezpieczeństwa
   - 4.1 Szkolenie i edukacja;
   - 4.2 Komunikacja w zakresie bezpieczeństwa.

### 8.4 ZAANGAŻOWANIE I ODPOWIEDZIALNOŚĆ ZARZĄDU

8.4.1 W każdej organizacji zarządzanie jest kontrolowaniem działalności personelu i wykorzystania zasobów, które są bezpośrednio związane lub konieczne dla realizacji usług. Wystawienie organizacji na zagrożenie bezpieczeństwa wynika z działań bezpośrednio związanych z dostawą usług. Poprzez konkretne działania personelu i wykorzystanie zasobów, kadra zarządzająca może aktywnie kontrolować ryzyko związane ze skutkami zagrożeń. Takie przykładowe działania to zatrudnianie, szkolenie i nadzorowanie przez kadrę zarządzającą pracowników, dostarczanie wyposażenia wspomagającego dostarczanie usługi. Kierownictwo musi być pewne, że pracownicy przestrzegają organizacyjnych wytycznych w zakresie bezpieczeństwa i kontroli, że wyposażenie z którego korzystają pozostaje w stanie gotowym do użycia. Pierwszoplanowa odpowiedzialność kierownictwa za zarządzanie bezpieczeństwem jest w ten sposób oczywista, a odpowiedzialność ta jest rozłożona poprzez działanie dedykowanego systemu, zawierającego wszystkie niezbędne kontrole zagrożenia bezpieczeństwa. SMS dostawcy usług oznacza wypełnienie tego zobowiązania. SMS jest systemem zarządzania zmierzającym do zapewnienia bezpiecznej i skutecznej działalności.

8.4.2 Punktem wyjścia do zapewnienia skuteczności i efektywności SMS w organizacji jest polityka bezpieczeństwa organizacji. Kierownictwo wyższego szczebla musi opracować politykę bezpieczeństwa podpisaną przez Dyrektora Odpowiedzialnego (*Accountable Executive*). Przykład polityki bezpieczeństwa jest zawarty w rysunku 8-1. Ogólnie rzecz biorąc, polityka bezpieczeństwa musi zawierać zobowiązanie do:

a) osiągnięcia najwyższych standardów bezpieczeństwa;

b) przestrzegania wszystkich obowiązujących wymogów prawnych i standardów międzynarodowych, i najbardziej skutecznych praktyk;

c) zapewnienia odpowiednich środków;

d) przestrzegania bezpieczeństwa jako podstawowego obowiązku całej kadry zarządzającej.

8.4.3 Informacje na temat polityki bezpieczeństwa muszą być przekazywane wszystkim pracownikom przy wyraźnym wsparciu ze strony kierownictwa wyższego szczebla.

8.4.4 Kierownictwo wyższego szczebla musi też ustalić cele związane z bezpieczeństwem, jak również standardy wykonania dla SMS, a tym samym dla całej organizacji. Cele związane z bezpieczeństwem muszą definiować co organizacja chce osiągnąć w zakresie zarządzania bezpieczeństwem oraz określić działania, które organizacja powinna podjąć, aby te cele osiągnąć. Standardy zapewnienia bezpieczeństwa pozwalają zmierzyć zachowania organizacji, w odniesieniu do wykonania działań w zakresie bezpieczeństwa, a zatem w stosunku do zarządzania bezpieczeństwem. Oba cele, zarówno w zakresie bezpieczeństwa, jak i wykonalności standardów bezpieczeństwa muszą być powiązane ze wskaźnikami wykonania działań w zakresie bezpieczeństwa, celami w zakresie bezpieczeństwa i planów działań SMS, omówionymi w rozdziale 6.

8.4.5 Organizacja musi wyznaczyć Dyrektora Odpowiedzialnego, który powinien być samodzielną, rozpoznawalną osobą, będącą ostatecznie odpowiedzialną za efektywne i skuteczne działanie SMS organizacji. Zależnie od wielkości i złożoności organizacji, osobą zarządzającą może być:

a) prezes zarządu;

b) dyrektor generalny;

c) partner; albo

d) właściciel.

8.4.6. Istnieje tendencja, aby określać, kto powinien zostać Dyrektorem Odpowiedzialnym, z punktu widzenia funkcji przypisanych do osoby w organizacji. Jednak ważniejsze niż to, kim powinien być Dyrektor Odpowiedzialny, są jego uprawnienia i odpowiedzialność w celu prawidłowej oceny poziomu wykonania założeń bezpieczeństwa SMS. Zakres uprawnień i odpowiedzialności obejmuje, ale nie ogranicza się do:

a) pełnej władzy w zakresie zasobów ludzkich;

b) pełnej władzy w zakresie głównych zagadnień finansowych;

c) bezpośredniej odpowiedzialności za prowadzenie spraw organizacji;

d) ostatecznej władzy nad operacjami certyfikowanymi;

e) ostatecznej odpowiedzialności za wszystkie kwestie bezpieczeństwa.

**DEKLARACJA BEZPIECZEŃSTWA**

Bezpieczeństwo to jedna z naszych podstawowych funkcji biznesowych. Jesteśmy zobowiązani do opracowywania, wdrażania, utrzymania i stałego poprawiania strategii i procesów w celu zapewnienia, że nasza działalność lotnicza odbywa się w warunkach zrównoważonej alokacji zasobów organizacji, ukierunkowanej na osiągnięcie najwyższego poziomu bezpieczeństwa oraz realizacji krajowych i międzynarodowych standardów świadczenia naszych usług.

Wszystkie szczeble zarządzania i wszyscy pracownicy, począwszy od Prezesa Zarządu (*chief executive officer (CEO)*) i Dyrektora Zarządzającego (managing director), są odpowiedzialni za zapewnienie najwyższego poziomu bezpieczeństwa.

Nasze zaangażowanie ma na celu:

- **Wsparcie** zarządzania bezpieczeństwem poprzez zapewnienie wszelkich właściwych środków, które mają doprowadzić do stworzenia kultury organizacyjnej, która będzie sprzyjać bezpiecznej pracy, zachęcać do skutecznej sprawozdawczości bezpieczeństwa i komunikacji, i aktywnie zarządzać innymi systemami w organizacji;

- **Egzekwowanie** zarządzania bezpieczeństwem jako podstawowego obowiązku całego kierownictwa i personelu;

- **Jasne określenie** dla wszystkich pracowników i kadry zarządzającej (managers) ich obowiązków i odpowiedzialności za realizację strategii bezpieczeństwa oraz działania naszego systemu zarządzania bezpieczeństwem;

- **Stworzenie i prowadzenie** procesów identyfikacji zagrożeń i zarządzania ryzykiem, w tym systemu raportowania zagrożeń, w celu wyeliminowania lub ograniczenia ryzyka wynikającego z zagrożeń, będących skutkiem naszej działalności operacyjnej, aż do osiągnięcia punktu, w którym ryzyko takie będzie utrzymywane na poziomie najniższym z możliwych (ALARP);

- **Zapewnienie**, że żadne konsekwencje nie zostaną wyciągnięte wobec żadnego pracownika, który poprzez system raportowania ujawnia zagrożenia dla bezpieczeństwa, chyba że takie ujawnienie wskazuje, ponad wszelką wątpliwość, działanie nielegalne, rażące zaniedbania lub umyślne lekceważenie przepisów lub procedur;

- **Wypełnianie** i w miarę możliwości przekraczanie ustawowych i prawnych wymogów i standardów;

- **Zapewnienie,** że dostępne są odpowiednio przeszkolone i wykwalifikowane zasoby ludzkie w celu realizacji strategii i polityki bezpieczeństwa;

- **Zapewnienie**, że wszyscy pracownicy otrzymują odpowiednie i stosowne informacje dotyczące bezpieczeństwa lotnictwa, właściwe szkolenie w sprawach bezpieczeństwa i, że przydzielono im wyłącznie zadania zgodne z posiadanymi przez nich umiejętnościami;

- **Określenie i analiza (pomiar)** realizacji naszych założeń w odniesieniu do realnych wskaźników bezpieczeństwa i celów działania w zakresie bezpieczeństwa;

- **Nieustanne ulepszanie** naszych działań w zakresie bezpieczeństwa poprzez procesy zarządzania, zapewniające podejmowanie odpowiednich i skutecznych kroków;

- **Zapewnienie**, że systemy i usługi firm zewnętrznych, które wspomagają nasze działania operacyjne i mają wpływ na poziom ich bezpieczeństwa, spełniają nasze standardy bezpieczeństwa.

(PODPIS) _____
Prezes Zarządu/ Dyrektor Zarządzający/ inna odpowiedzialna osoba
CEO/Managing Director/or as appropriate

**Ilustracja 8-1. Przykład polityki bezpieczeństwa**

8.4.7 Rozdział 2 omawia sposób alokacji zasobów jako podstawowy proces w organizacji. Przydział środków jest zatem jedną z pierwotnych funkcji zarządzania. Paragraf 8.4.1 omawia funkcję zarządzania, jako jedną z funkcji kontroli działania pracowników i wykorzystania zasobów, bezpośrednio związanych z dostawą usług, w wyniku których organizacja jest wystawiona na zagrożenia bezpieczeństwa. W związku z powyższym stanowi to podstawę, która uzasadnia zakres odpowiedzialności i uprawnień Dyrektora Odpowiedzialnego, o którym mowa w paragrafie 8.4.6: taka odpowiedzialność i uprawnienia odnoszą się zarówno do alokacji zasobów, jak i kontroli działalności. Dyrektor Odpowiedzialny, który jeśli nie otrzyma takich uprawnień i odpowiedzialności, nie będzie mógł właściwie sprawować swoich funkcji.

8.4.8 Dyrektor Odpowiedzialny może wyznaczyć inną osobę do zarządzania systemem bezpieczeństwa, pod warunkiem, że wyznaczenie takiej osoby jest odpowiednio udokumentowane i opisane w organizacji, w podręczniku systemu zarządzania bezpieczeństwem (SMSM), co jest omówione w dalszej części niniejszego rozdziału. Jednakże przeniesienie zarządzania SMS na inną osobę, nie zwalnia Dyrektora Odpowiedzialnego z ostatecznej odpowiedzialności za działanie SMS w organizacji.

## 8.5 ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO

8.5.1 W Rozdziale 3 opisano zarządzanie bezpieczeństwem jako podstawową funkcję biznesową, która wspomaga analizę zasobów organizacji i jej celów. Analiza ta stanowi z kolei podstawę do wyważonego i realnego podziału środków pomiędzy ochronę i cele produkcyjne, które wspomagają ogólne potrzeby organizacji w zakresie świadczenia usług. Paragraf 8.4.1 opisuje SMS jako system zarządzania w celu zapewnienia bezpieczeństwa wykonywanych operacji. Bezpieczne wykonywanie operacji jest mało prawdopodobne, bez pewności, że zrównoważony i realny podział środków pomiędzy celami ochrony i produkcji, wspierający ogólne potrzeby organizacji w zakresie świadczenia usług został osiągnięty. Ogólnie rzecz biorąc, odpowiedzialność za zapewnienie bezpieczeństwa wykonywanych operacji oraz osiągnięcie równowagi i realizm w alokacji zasobów, urzeczywistnia się niezależnie od organizacji SMS, w szczególności poprzez jeden konkretny element SMS: definicję odpowiedzialności w zakresie bezpieczeństwa całego personelu, a przede wszystkim kluczowych pracowników.

8.5.2 Odpowiedzialność menedżerów za bezpieczeństwo w zakresie organizacji SMS odnosi się do definicji struktury organizacji SMS, która odpowiada wielkości, rodzajowi i stopniu złożoności operacji oraz niebezpieczeństw i zagrożeń bezpieczeństwa związanych z działaniami niezbędnymi do świadczenia usług. Odpowiedzialność menedżerów za bezpieczeństwo w zakresie organizacji SMS zawiera także alokację zasobów ludzkich, technicznych, finansowych lub jakichkolwiek innych środków niezbędnych do skutecznego i wydajnego działania SMS.

8.5.3 Chociaż zakresy czynności wszystkich pracowników, niezależnie od szczebla, powinny zawierać zakresy obowiązków i odpowiedzialności za bezpieczeństwo, to odpowiedzialność za bezpieczeństwo w odniesieniu do definicji i uprawnień kluczowego personelu, odnosi się też do opisu czynności pracy na stanowisku kierowniczym (szefa działu lub osoby odpowiedzialnej za funkcjonowanie komórki organizacyjnej) i obowiązków w zakresie funkcjonowania SMS. Z perspektywy zarządzania bezpieczeństwem jako podstawowej funkcji biznesowej, każdy szef działu lub osoba odpowiedzialna za jednostkę funkcjonalną będzie zaangażowana w działanie SMS i jej wyników w zakresie bezpieczeństwa. Zaangażowanie takie będzie na pewno głębsze u osób odpowiedzialnych za działania służb lub jednostek funkcjonalnych bezpośrednio odpowiedzialnych za dostarczanie podstawowych usług organizacji (działalność operacyjna, utrzymanie, usługi techniczne, szkoleniowe i odprawa, określanych zwyczajowo jako „kierownicy liniowi") niż dla osób odpowiedzialnych za wspieranie funkcji (zasoby ludzkie, administracja, usługi prawne i finansowe).

8.5.4 Odpowiedzialność w zakresie bezpieczeństwa, obowiązki i uprawnienia wszystkich kierowników działów i/lub osób odpowiedzialnych za komórki organizacyjne, a w szczególności kierowników liniowych, muszą być opisane w instrukcji systemów zarządzania bezpieczeństwem organizacji (SMSM), która zostanie omówiona w dalszej części tego rozdziału. Odpowiedzialność w zakresie bezpieczeństwa, obowiązki i uprawnienia muszą być przedstawione graficznie, w postaci wykresu ukazującego linie styku i wzajemne relacje między różnymi sektorami organizacji w warunkach zarządzania bezpieczeństwem. Przykładem takiego funkcjonalnego wykresu jest Rysunek 8-2.

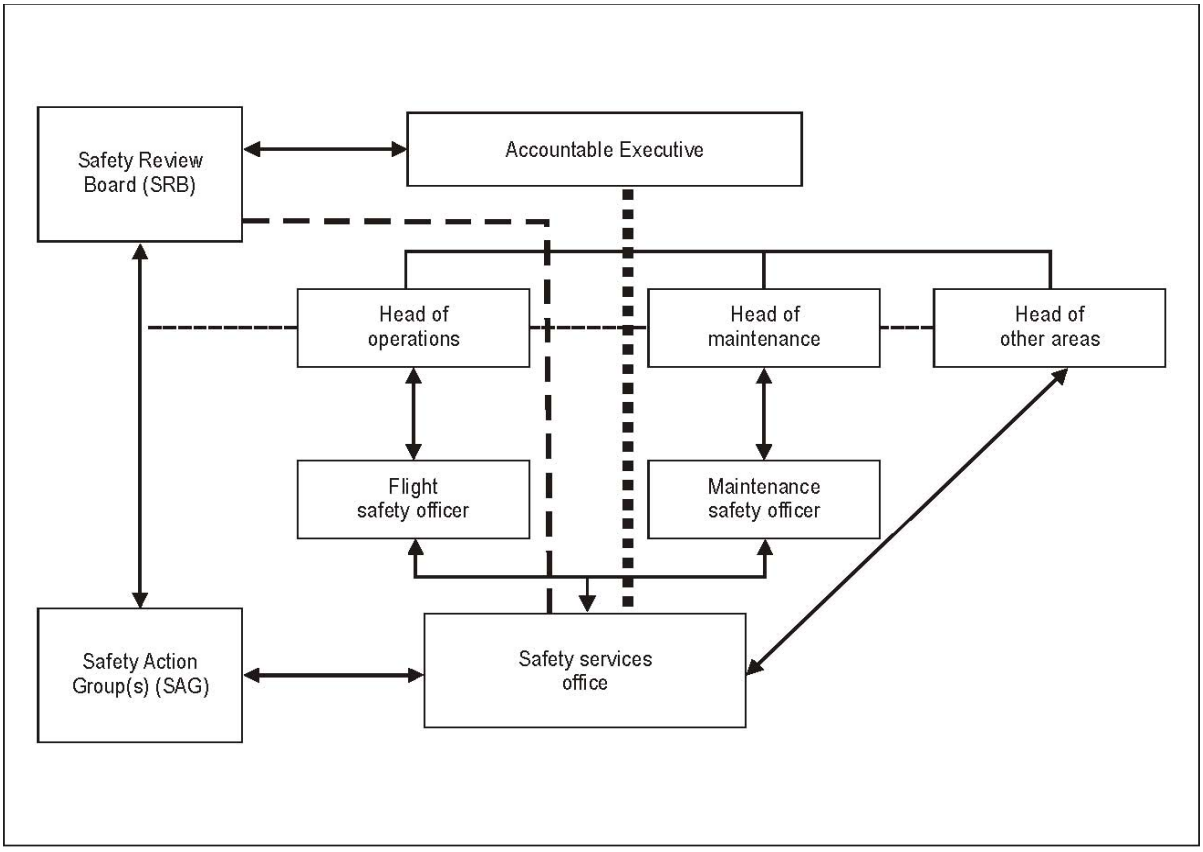



**Figure 8-2. Safety accountabilities**

8.5.5 Należy pamiętać, że Rysunek 8-2 przedstawia funkcje, a nie schemat organizacji. Nie jest on przeznaczony dla zobrazowania zarządzania bezpieczeństwem w organizacji w odniesieniu do służb i jednostek funkcjonalnych i ich względnej pozycji w hierarchii przedsiębiorstwa. Przedstawia funkcje każdego działu i /lub komórek organizacyjnych w zakresie zapewnienia bezpieczeństwa jako podstawowych procesów biznesowych. To zastrzeżenie jest istotne, ponieważ liczba możliwych schematów będzie tak duża, jak wiele organizacji istnieje w dziedzinie lotnictwa. Dlatego też, dla celów tego podręcznika, rys. 8-2 musi być traktowany jako schemat funkcjonalny, a nie jako schemat organizacyjny.

8.5.6 Biuro ds. bezpieczeństwa znajduje się w centrum funkcjonalnego wykresu. Koncepcja takiego biura jest kluczem do zrozumienia zasad zarządzania bezpieczeństwem w podstawowych procesach biznesowych i zrozumienia SMS, jako systemu wykorzystywanego do tego celu przez personel zarządzający. Biuro ds. bezpieczeństwa jest niezależne i neutralne pod względem procesów i decyzji wydawanych w zakresie świadczenia usług przez kierowników liniowych z jednostek operacyjnych. W środowisku SMS, biuro ds. bezpieczeństwa spełnia cztery podstawowe funkcje przedsiębiorstw:

a) zarządza i nadzoruje system identyfikacji zagrożeń;

b) monitoruje poziom bezpieczeństwa jednostek operacyjnych bezpośrednio zaangażowanych w świadczenie usług;

c) doradza kierownictwu wyższego szczebla w sprawach zarządzania bezpieczeństwem;

d) wspiera kierowników liniowych w sprawach zarządzania bezpieczeństwem.

8.5.7 W tradycyjnym podejściu do zagadnień dotyczących bezpieczeństwa, biuro ds. bezpieczeństwa, omówione w rozdziale 2, było wyłącznym "właścicielem" całego procesu zapewniania bezpieczeństwa w organizacji. Pracownik ds. bezpieczeństwa, często określany jako urzędnik do zapobiegania wypadkom (*accident prevention officer*), był osobą odpowiedzialną za identyfikację problemów związanych z bezpieczeństwem, proponowanie i udział we wdrażaniu rozwiązań, a także monitorowanie ich skuteczności. W ostatnich latach, pogląd odnośnie "własności" procesu zapewnienia bezpieczeństwa, ograniczonego wyłącznie do biura ds. bezpieczeństwa, powoli zmieniał się na rzecz powszechnie przyjętej praktyki branżowej ustanawiającej bezpośrednie raportowanie i przekazywanie informacji pomiędzy pracownikiem ds. bezpieczeństwa a Prezesem organizacji.

8.5.8 Istniały dwojakie przyczyny upowszechniania powyższej praktyki. Pierwsza miała na celu umiejscowienie biura ds. bezpieczeństwa wyżej w strukturze organizacyjnej poprzez ustanowienie bezpośredniej zależności między biurem ds. bezpieczeństwa i Zarządem. Druga polegała na wykorzystaniu bezpośredniej podległości biura, w celu stworzenia jego neutralności poprzez wyeliminowanie kierowników liniowych, odpowiedzialnych za zarządzanie działalnością operacyjną związaną bezpośrednio ze świadczeniem usług, z oceny i rozwiązywania problemów dotyczących bezpieczeństwa. Takie podejście wynikało z dużego prawdopodobieństwa, że kierownicy liniowi mogliby stać się, w różnym stopniu, stroną przy ocenie i rozwiązywaniu problemów bezpieczeństwa. Mogłoby to prowadzić do potencjalnego konfliktu interesów. Bezpośrednią relację pomiędzy urzędnikiem ds. bezpieczeństwa a Zarządem wprowadzono, aby usunąć potencjalny konflikt interesów.

8.5.9 Praktyka ta, pomimo, że wynikała z dobrych intencji, posiadała jednak dwie poważne wady. Po pierwsze, poprzez nałożenie odpowiedzialności za procesy bezpieczeństwa wyłącznie na biuro ds. bezpieczeństwa, odsunięto, od podejmowania decyzji w zakresie bezpieczeństwa, kierowników liniowych. Wytworzyło to przekonanie, że problemy dot. bezpieczeństwa były problemami kierowników liniowych, a problemy związane z bezpieczeństwem należały do biura ds. bezpieczeństwa i pracownika ds. bezpieczeństwa. Granica odpowiedzialności została zatem skutecznie zredukowana do dwustronnego dialogu pomiędzy Prezesem a pracownikiem ds. bezpieczeństwa. Biorąc pod uwagę obciążenia Zarządu różnymi obowiązkami, dialog ten miał w sobie potencjał do przerodzenie się w monolog. Po drugie, i najważniejsze, rozwiązanie takie wykluczało cenny wkład w zakresie wiedzy praktycznej („know-how”), którą wydziały operacyjne mogłyby wnieść w proces decyzyjny odnośnie bezpieczeństwa organizacji.

8.5.10 Środowisko SMS stwarza inną perspektywę. Nazwę biuro ds. bezpieczeństwa zmieniono na biuro usług ds. bezpieczeństwa (*Safety Services Office*). Zmiana ta pokazuje, że ma ono za zadanie świadczyć usługi na rzecz całej organizacji, w tym kierowników wyższego szczebla i kierowników liniowych, w zakresie zarządzania bezpieczeństwem będącym podstawowym procesem biznesowym organizacji. Aforyzm mówiący, że "nie można zarządzać czymś, czego się nie zmierzy" omówiony w rozdziale 3 jest skierowany do SMS. Biuro usług ds. bezpieczeństwa jest zasadniczo zbiorem danych dotyczących bezpieczeństwa i analizy jednostki. Dzięki kombinacji metod prognozującej, proaktywnej i reaktywnej (omawianych w Rozdziale 3) biuro usług ds. bezpieczeństwa odpowiada za działalność organizacji w obszarze operacyjnym (również omówione w rozdziale 3) poprzez stałe i rutynowe gromadzenie danych odnośnie poziomu bezpieczeństwa w sytuacji zagrożeń podczas świadczenia usług.

8.5.11 Po identyfikacji zagrożeń i ocenie ich skutków dla bezpieczeństwa oraz oszacowaniu ryzyka dla bezpieczeństwa tych skutków (np. gdy informacje odnośnie bezpieczeństwa zostały wygenerowane z bazy danych), informacje dotyczące bezpieczeństwa są dostarczane do kierowników liniowych w celu zaproponowania rozwiązania. Ponieważ kierownicy liniowi są w swoich dziedzinach ekspertami, będą w stanie najlepiej ocenić skuteczność i efektywność rozwiązań i sposób ich realizacji. Kierownicy liniowi ponadto są w stanie podjąć ostateczne kroki w procesie analizowania danych, przetwarzając informacje z zakresu bezpieczeństwa w informacje o charakterze poufnym, wprowadzając do kontekstu informacje o zagrożeniach, przefiltrowane przez biuro usług ds. bezpieczeństwa.

8.5.12 Podobnie jak w całej organizacji, podstawowa odpowiedzialność za zarządzanie bezpieczeństwem spoczywa na tych, do których „należy” działalność produkcyjna. Ma to miejsce w trakcie działalności produkcyjnej, podczas której organizacja bezpośrednio styka się z zagrożeniami, gdy nieprawidłowości w procesach organizacyjnych przyczyniają się do uwolnienia szkodliwych skutków zagrożeń i gdzie przez bezpośredni nadzór, kontrolę i alokację zasobów można zminimalizować to zagrożenie do ALARP. Ponadto, „właściciele” procesu są w każdej organizacji formalnymi ekspertami w swoich dziedzinach, a co za tym idzie posiadają największą wiedzę na temat technologicznych procesów produkcji.

8.5.13 Po dostarczeniu informacji odnośnie bezpieczeństwa do odpowiednich kierowników liniowych, biuro usług ds. bezpieczeństwa wznawia rutynowe gromadzenie danych odnośnie bezpieczeństwa i analizę działalności. W uzgodnionych, pomiędzy biurem usług ds. bezpieczeństwa kierownikami liniowymi, przedziałach czasowych, biuro usług ds. bezpieczeństwa przedstawi kierownikom liniowym nowe informacje na temat obaw odnośnie poziomu bezpieczeństwa w obszarach, których takie zagrożenie dotyczy. Informacja ta wykaże, czy rozwiązania wprowadzone przez menedżerów liniowych łagodzące zagrożenie bezpieczeństwa zostały właściwie

ukierunkowane lub gdy obawy odnośnie poziomu bezpieczeństwa nie ustępują. W drugim przypadku, podejmowane będą dalsze rozwiązania, uzgadniany nowy interwał czasowy, gromadzone i analizowane są dane dotyczące bezpieczeństwa, dostarczana jest informacja dotycząca poziomu bezpieczeństwa i cykl ten powtarzany jest do momentu, w którym wynik analizy wskaże, że zagrożenie dla bezpieczeństwa zostało usunięte. W trakcie tego procesu, kierownicy liniowi nie raportują do biura usług ds. bezpieczeństwa, ale do Dyrektora Odpowiedzialnego, osoby ostatecznie odpowiedzialnej za SMS organizacji, za pośrednictwem jednego z dwóch formalnych organów bezpieczeństwa omówionych w rozdziale 8.6.

## 8.6 WYZNACZENIE KLUCZOWEGO PERSONELU ODPOWIEDZIALNEGO ZA BEZPIECZEŃSTWO

8.6.1 Kluczem do skutecznego wdrożenia i funkcjonowania biura usług ds. bezpieczeństwa jest wyznaczenie osoby odpowiedzialnej za codzienne funkcjonowanie tego biura. Osoba ta może być różnie nazywana w różnych organizacjach, ale dla celów tego podręcznika zachowana zostanie pierwotna nazwa Dyrektor ds. bezpieczeństwa (*safety manager*).

8.6.2 Dyrektorem ds. bezpieczeństwa w większości organizacji, będzie osoba, której Dyrektor Zarządzający (Accountable Executive) wyznaczył funkcje stałego zarządzania SMS. Dyrektor ds. bezpieczeństwa jest osobą odpowiedzialną i centralną za rozwój i utrzymania efektywnego SMS. Dyrektor ds. bezpieczeństwa doradza również Dyrektorowi Zarządzającemu (*Accountable Executive*) i kierownikom liniowym w sprawach związanych z zarządzaniem bezpieczeństwem i jest odpowiedzialny za koordynację i przekazywanie informacji dotyczących spraw bezpieczeństwa w ramach organizacji, jak również zewnętrznym agencjom, kontrahentom i udziałowcom, jeśli ma to zastosowanie. Funkcje Dyrektora ds. bezpieczeństwa obejmują, ale nie ograniczają się do:

a) kierowania planem wdrażania SMS w imieniu Dyrektora Zarządzającego;

b) prowadzenia/ułatwiania identyfikacji zagrożeń i analizy ryzyka w zakresie bezpieczeństwa;

c) monitorowania działań korygujących i oceny ich wyników;

d) zapewnienia okresowego raportowania na temat poziomu bezpieczeństwa organizacji;

e) prowadzenia ewidencji i dokumentacji w zakresie bezpieczeństwa;

f) planowania i organizowanie szkoleń pracowników w zakresie bezpieczeństwa;

g) świadczenia niezależnego doradztwa w sprawach bezpieczeństwa;

h) monitorowania zagrożeń dla bezpieczeństwa w przemyśle lotniczym i obserwowanie ich wpływu na działania organizacji skierowane na dostarczanie usług;

i) koordynacji i komunikowania się (w imieniu *Accountable Executive*) w sprawach dotyczących bezpieczeństwa z państwowym organem nadzoru i innymi instytucjami państwowymi; i

j) koordynowania i komunikowania się (w imieniu *Accountable Executive*) w sprawach dotyczących bezpieczeństwa z agencjami międzynarodowymi.

8.6.3 Dyrektor ds. bezpieczeństwa może być pojedynczą osobą prowadzącą biuro usług ds. bezpieczeństwa lub może być wspierany przez dodatkowych pracowników, w większości analityków danych. Będzie to zależeć od wielkości organizacji, charakteru i złożoności działań wspierających świadczenie usług. Niezależnie od wielkości biura ds. bezpieczeństwa i poziomu zatrudnienia, jego funkcje pozostają takie same. Dyrektor ds. bezpieczeństwa współpracuje bezpośrednio z kierownikami liniowymi (działalność operacyjna, utrzymanie, technika, szkolenie itp.). Jest to pokazane na wykresie funkcjonalnym przy pomocy strzałek, na rysunku 8-2. Jeżeli, ze względu na wielkość organizacji, szefowie wydziałów operacyjnych dysponują dedykowanym pracownikiem ds. bezpieczeństwa, ze specjalistyczną wiedzą w przedmiotowych sprawach i delegowanym zakresem odpowiedzialności za zarządzanie problemami związanymi z bezpieczeństwem na danym obszarze, wówczas będzie on pierwszym punktem kontaktowym dla Dyrektora ds. bezpieczeństwa.

8.6.4 W normalnych warunkach, Dyrektor ds. bezpieczeństwa uzyskuje dostęp i/lub komunikuje się z Dyrektorem Zarządzającym (*Accountable Executive*) poprzez: Grupę Reagowania ds. bezpieczeństwa (*Safety Action Group*) i dalej przez Komisję ds. Przeglądu Bezpieczeństwa (*Safety Review Board*) lub bezpośrednio przez Komisję ds. Przeglądu Bezpieczeństwa. Grupy te są omówione w dalszej części niniejszego rozdziału.

W sytuacjach wyjątkowych lub nagłych, Dyrektor ds. bezpieczeństwa musi mieć bezpośredni, awaryjny dostęp do Dyrektora Zarządzajacego (*Accountable Executive*), zgodnie z narysowaną na wykresie kropkowaną linią łączącą odpowiednie pola, rysunek 8-2. Ten kanał komunikacji powinien być wykorzystywany rzadko, a gdy tak się stanie, powinno być to odpowiednio uzasadnione i udokumentowane.

8.6.5 W środowisku SMS, Dyrektor ds. bezpieczeństwa jest osobą odpowiedzialną za zbieranie i analizę danych na temat zagrożeń bezpieczeństwa i dystrybucję wśród kierowników liniowych informacji na temat zagrożeń bezpieczeństwa i ryzyka związanego ze skutkami tych zagrożeń. Sam w sobie, Dyrektor ds. bezpieczeństwa często jest niejako „zwiastunem" złych wiadomości. W związku z tym kryteria jego wyboru nabierają szczególnego znaczenia i powinny obejmować, lecz nie ograniczać się do następujących elementów:

a) doświadczenia w zarządzaniu operacyjnym;

b) doświadczenia technicznego potrzebnego do zrozumienia działania systemów wspomagających operacje;

c) zdolności w zakresie kontaktów interpersonalnych;

d) zdolności analitycznych i umiejętność rozwiązywania problemów;

e) umiejętności zarządzania projektami;

f) umiejętności komunikowania się w formie pisemnej i ustnej.

*Uwaga. - przykładowy opis stanowiska dla Dyrektora ds. bezpieczeństwa został zawarty w Dodatku 2 do niniejszego rozdziału.*

8.6.6 Rozpowszechnianie informacji na temat zagrożeń bezpieczeństwa i ryzyka związanego ze skutkami tych zagrożeń przez biuro ds. usług bezpieczeństwa jest tylko pierwszym krokiem w procesie zarządzania ryzykiem. Informacja ta musi być odebrana przez kierowników liniowych. Łagodzenie zagrożeń w zakresie bezpieczeństwa bezwzględnie wymaga zasobów. Zasoby takie czasami są dostępne bezpośrednio kierownikom liniowym. Często jednak wymagane są dodatkowe zasoby, których podział nie jest możliwy na poziomie kierowników liniowych, ale muszą być one zatwierdzone przez wyższy szczebel kierowniczy organizacji. Również potrzebne jest istnienie w organizacji jakiegoś formalnego procesu mającego na celu zapewnienie obiektywności w ocenie skuteczności i efektywności strategii łagodzenia skutków w stosunku do uzgodnionego poziomu bezpieczeństwa organizacji. Komisja ds. przeglądu bezpieczeństwa (SRB) stanowi platformę do osiągania celów związanych z alokacją zasobów i bezstronnej oceny skuteczności i efektywności strategii łagodzenia skutków.

8.6.7 Komisja ds. przeglądu bezpieczeństwa (SRB) jest komitetem na bardzo wysokim szczeblu kierowania, w skład którego wchodzą kierownicy wyższego szczebla, w tym dyrektorzy odpowiedzialni za obszary funkcjonalne, a któremu przewodniczy Dyrektor Zarzadzający (*Accountable Executive*). Dyrektor ds. bezpieczeństwa uczestniczy w SRB tylko z głosem doradczym. SRB jest wybitnie strategicznym ciałem, zajmującym się tematami z zakresu polityki organizacji, alokacji zasobów i monitorowania realizacji działań organizacji, spotyka się rzadko, chyba że wyjątkowe okoliczności wymuszą inne działanie. Komisja ds. przeglądu bezpieczeństwa (SRB):

a) monitoruje skuteczność planu implementacji SMS;

b) monitoruje czy konieczne działania naprawcze są podjęte w odpowiednim czasie;

c) monitoruje poziom bezpieczeństwa w stosunku do polityki bezpieczeństwa i celów organizacji;

d) monitoruje skuteczność procesów zarządzania bezpieczeństwem w organizacji wspierając deklarowane przez firmę priorytety zarządzania bezpieczeństwem jako podstawowego procesu biznesowego;

e) monitoruje skuteczność nadzoru w zakresie bezpieczeństwa zleconych operacji;

f) zapewnia, że odpowiednie zasoby są alokowane w sposób pozwalający osiągnąć poziom bezpieczeństwa jaki wymaga przestrzeganie przepisów;

g) zapewnia kierownictwo strategiczne grupy reagowania ds. bezpieczeństwa (SAG).

8.6.8 Po opracowaniu przez Komisję ds. przeglądu bezpieczeństwa (SRB) kierunku, wspólne wdrożenie strategii w całej organizacji musi odbywać się w sposób skoordynowany. Jest to podstawową rolą grupy reagowania ds. bezpieczeństwa (SAG). SAG stanowi komitet, stojący wysoko w hierarchii organizacyjnej, złożony z kierowników i przedstawicieli pracowników front-line, pod przewodnictwem wyznaczonych kolejno kierowników. Dyrektor ds. bezpieczeństwa jest sekretarzem SAG. SAG jest ciałem wybitnie taktycznym i zajmującym się problemami związanymi z wdrażaniem strategicznych dyrektyw SRB. Podczas gdy SAG zajmuje się sprawami implementacji na "poziomie przeciętnych ludzi" odnosząc się do realizacji konkretnych działań w celu zapewnienia kontroli zagrożeń bezpieczeństwa i ryzyka związanego ze skutkami tych zagrożeń w czasie operacji liniowych, SRB zajmuje się koordynacją tych zagadnień, w celu zapewnienia spójności ze strategicznym kierunkiem nakreślonym przez SRB.
SAG:

a) nadzoruje wyniki działalności operacyjnej w zakresie bezpieczeństwa w obszarach funkcjonalnych i zapewnia, że identyfikacja zagrożeń i zarządzanie ryzykiem będą w razie potrzeby przeprowadzane z udziałem pracowników, których uczestnictwo jest niezbędne do budowania świadomości w zakresie bezpieczeństwa;

b) koordynuje rozwiązania strategii łagodzenia skutków zidentyfikowanych zagrożeń i zapewnia, że istnieją zadowalające warunki gromadzenia danych z zakresu bezpieczeństwa i opinii pracowników;

c) ocenia wpływ zmian operacyjnych na poziom bezpieczeństwa;

d) koordynuje realizację planu działań korygujących i zwołuje posiedzenia lub spotkania informacyjne w zakresie niezbędnym do zapewnienia, że istnieją duże możliwości dla wszystkich pracowników do pełnego uczestnictwa w zarządzaniu bezpieczeństwem;

e) zapewnia, że w odpowiednim czasie zostaną podjęte działania naprawcze;

f) ocenia skuteczność dotychczasowych zaleceń dotyczących bezpieczeństwa;

g) nadzoruje promowanie bezpieczeństwa i zapewnia, że odpowiednie szkolenie personelu w zakresie bezpieczeństwa, ratownictwa, obsługi technicznej przeprowadzane jest zgodnie z minimalnymi wymogami.

## 8.7 KOORDYNACJA REAGOWANIA W SYTUACJI AWARYJNEJ

8.7.1 Plan działań kryzysowych (ERP) określa na piśmie, jakie działania należy podjąć po wypadku i kto jest odpowiedzialny za dane działanie. Celem ERP jest zapewnienie, że nie ma prawidłowego i skutecznego przejścia od normalnych do nadzwyczajnych działań, włączając delegowanie uprawnień i podział obowiązków w sytuacji awaryjnej. Upoważnienie do podejmowania działań przez kluczowy personel jest zawarte również w planie, a także koordynacji wysiłków na rzecz sprostania sytuacji kryzysowej. Celem ogólnym jest bezpieczne kontynuowanie operacji lub jak najszybszy powrót do normalnych operacji.

8.7.2 Porty lotnicze są zobowiązane opracować lotniskowy plan ratownictwa (AEP), służby ruchu lotniczego muszą opracować plan wariantowy, a linie lotnicze muszą opracować plan reagowania w sytuacjach awaryjnych. Ponieważ porty lotnicze, kontroli ruchu lotniczego i operacje lotnicze zazębiają się, jasne jest, że plany te powinny być kompatybilne. Koordynacja tych planów powinna być opisana w instrukcji SMS.

## 8.8 DOKUMENTACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM

8.8.1 Jak opisano w rozdziale 7, jedną z wyraźnych cech SMS jest to, że wszystkie czynności zarządzania bezpieczeństwem muszą być udokumentowane i widoczne, a zatem dokumentacja jest niezbędnym elementem SMS.

8.8.2 Dokumentacja SMS musi zawierać i odnosić się, w stosownych przypadkach, do wszystkich odpowiednich i stosowanych krajowych i międzynarodowych regulacji. Do dokumentacji muszą być także włączone zapisy specyficzne dla SMS i dokumenty takie jak formularze dotyczące raportowania zagrożeń, granic odpowiedzialności, odpowiedzialności i uprawnień w zakresie zarządzania bezpieczeństwem operacyjnym i struktura organizacji zarządzania bezpieczeństwem. Ponadto należy także dokumentować wytyczne do zarządzania dokumentami, a w tym magazynowania, pobierania i konserwacji. Ale bez wątpienia najważniejszą składową dokumentacji jest podręcznik systemu zarządzania bezpieczeństwem organizacji (SMSM).

8.8.3 SMSM jest narzędziem kluczowym służącym do komunikowania podejścia całej organizacji do problematyki bezpieczeństwa. Podręcznik dokumentuje wszystkie aspekty SMS, włączając politykę bezpieczeństwa, cele, procedury i indywidualną odpowiedzialność za bezpieczeństwo.

8.8.4 SMSM standardowo zawiera poniższe informacje:

a) zakres systemu zarządzania bezpieczeństwem;

b) politykę bezpieczeństwa i jej cele;

c) odpowiedzialność za bezpieczeństwo;

d) personel kluczowy dla zapewnienia bezpieczeństwa;

e) dokumentacja procedur kontroli;

f) koordynacja planów reagowania w sytuacjach awaryjnych;

g) identyfikacja ryzyka i plan zarządzania ryzykiem;

h) zapewnienie bezpieczeństwa;

i) monitorowanie realizacji działań w zakresie bezpieczeństwa;

j) kontrola bezpieczeństwa;

k) zarządzanie zmianami;

l) promowanie bezpieczeństwa;

m) działalność zlecana.

### 8.9 PLAN WDROŻENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM

8.9.1 Plan wdrożenia SMS określa podejście organizacji do zarządzania bezpieczeństwem. Jako taki jest realistyczną strategią wdrożenia SMS spełniającego cele bezpieczeństwa organizacji przy jednoczesnym wspieraniu skutecznej i efektywnej realizacji usług. Strategia ta opisuje, w jaki sposób organizacja będzie osiągać swoje cele w zakresie bezpieczeństwa i jak będzie wypełniać wszystkie nowe lub zmienione wymogi dotyczące bezpieczeństwa. Znaczące pozycje w tym planie zazwyczaj są włączane do biznes planu organizacji. Plan wdrożenia programu SMS, który może składać się z więcej niż jednego dokumentu, specyfikuje jakie działania należy podjąć, przez kogo i w jakim terminie.

8.9.2 W zależności od wielkości organizacji i złożoności prowadzonej przez nią działalności, plan wdrożenia SMS może być opracowany przez jedną osobę lub przez grupę planowania, która posiada odpowiednie doświadczenie bazowe. Grupa planowania powinna spotykać się regularnie z kadrą kierowniczą wyższego szczebla w celu oceny postępów w realizacji planu i przyznania odpowiednich zasobów (włączając czas na spotkania) proporcjonalnych do realizacji zadań.

8.9.3 Plan wdrażania programu SMS standardowo zawiera następujące elementy:

a) politykę bezpieczeństwa i jej cele;

b) opis systemu;

c) analizę luk;

d) składowe SMS;

e) funkcje bezpieczeństwa i odpowiedzialność;

f) politykę zgłaszania zagrożeń;

g) sposoby angażowania pracowników;

h) ocenę wyników w zakresie bezpieczeństwa;

i) komunikat bezpieczeństwa;

j) szkolenie w zakresie bezpieczeństwa;

k) omówienie zarządzania poziomu realizacji bezpieczeństwa.

8.9.4 Opracowany plan wdrożenia SMS musi zostać zatwierdzony przez wyższy szczebel kierowniczy. Przeciętne ramy czasowe realizacji SMS wynoszą od roku do czterech lat. Wdrażanie programu SMS uwzględniające poszczególne fazy zostało omówione w Rozdziale 10, a wytyczne dotyczące metodologii opracowywania planu wdrażania SMS i harmonogramu znajdują się w Dodatku 2 do tego rozdziału.

## Dodatek 1 do Rozdziału 8

# RAMY SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM (SMS)

SMS jest narzędziem zarządzania w zakresie zarządzania bezpieczeństwem w organizacji. Ten Dodatek określa ramy wdrożenia i utrzymania systemu zarządzania bezpieczeństwem (SMS) przez organizację. Obszar zakresu powinien być proporcjonalny do wielkości organizacji i złożoności świadczonych usług. Ramy obejmują cztery części i dwanaście elementów, co stanowi minimalne wymagania dla realizacji SMS.

1. Polityka bezpieczeństwa oraz jej cele
    - 1.1 Zaangażowanie kierownictwa i jego odpowiedzialność kierownicza
    - 1.2 Odpowiedzialność za bezpieczeństwo
    - 1.3 Powołanie kluczowego personelu ds. bezpieczeństwa
    - 1.4 Koordynacja planowania w sytuacjach kryzysowych
    - 1.5 Dokumentacja SMS
2. Zarządzanie ryzykiem
    - 2.1 Identyfikacja zagrożeń
    - 2.2 Ocena ryzyka i jego minimalizowanie
3. Zapewnienie bezpieczeństwa
    - 3.1 Monitorowanie poziomu bezpieczeństwa i pomiar
    - 3.2 Zarządzanie zmianami
    - 3.3 Ciągłe doskonalenie i wdrażanie systemu zarządzania
4. Propagowanie bezpieczeństwa
    - 4.1 Szkolenie i edukacja
    - 4.2 Komunikacja w zakresie bezpieczeństwa.

### 1. POLITYKA BEZPIECZEŃSTWA ORAZ JEJ CELE

#### 1.1 Zaangażowanie kierownictwa i jego odpowiedzialność kierownicza

[Organizacja] określa politykę bezpieczeństwa, która będzie zgodna z wymogami międzynarodowymi i krajowymi i jest podpisana przez najwyższego zwierzchnika tej organizacji. Polityka bezpieczeństwa odzwierciedla zobowiązania organizacyjne dotyczące bezpieczeństwa; zawiera wyraźne oświadczenie o zapewnieniu niezbędnych środków dla realizacji polityki bezpieczeństwa oraz została ogłoszona w całej organizacji. Polityka bezpieczeństwa obejmuje procedury przekazywania informacji oraz wyraźnie wskazuje, które rodzaje czynności operacyjnych są niedopuszczalne, a także określa warunki, w których nie będzie się wszczynać postępowania dyscyplinarnego. Polityka bezpieczeństwa podlega okresowym przeglądom w celu upewnienia się, że jest nadal aktualna i odpowiednia dla organizacji.

#### 1.2 Odpowiedzialność za bezpieczeństwo

[Organizacja] określa Osobę odpowiedzialną, która niezależnie od innych funkcji, ma w imieniu [organizacji] najwyższą odpowiedzialność i kompetencje do wdrożenia i utrzymywania SMS. [Organizacja] określa również zakres odpowiedzialności wszystkich członków zarządu niezależnie od ich innych pełnionych funkcji, jak również określa zakres odpowiedzialności pracowników w odniesieniu do SMS. Zadania w zakresie bezpieczeństwa, zakresy odpowiedzialności za bezpieczeństwo oraz uprawnienia są udokumentowane i zakomunikowane całej

organizacji i obejmują definicję poziomów zarządzania z uprawnieniami do podejmowania decyzji w zakresie tolerancji zagrożeń.

### 1.3 Powołanie kluczowego personelu ds. bezpieczeństwa

[Organizacja] powołuje dyrektora ds. bezpieczeństwa odpowiedzialnego indywidualnie za bezpieczeństwo będącego jednocześnie centralną jednostką dla wdrożenia i utrzymania skutecznego SMS.

### 1.4 Koordynacja planowania w sytuacjach kryzysowych

[Organizacja] zapewnia, że plan reagowania kryzysowego, który przewiduje skuteczne i prawidłowe przejście od sytuacji normalnej do działań nadzwyczajnych, a następnie powrotu do normalnych czynności jest właściwie skoordynowany z planami reagowania kryzysowego innych organizacji i służb, które również świadczą swoje usługi i wykonują swoje czynności.

### 1.5 Dokumentacja SMS

[Organizacja] opracuje plan wdrożenia SMS, zatwierdzony przez kierownictwo wyższego szczebla organizacji, który określi podejście organizacji do zarządzania bezpieczeństwem w sposób, który spełnia założone cele w zakresie bezpieczeństwa. [Organizacja] rozwija i prowadzi dokumentację SMS, która opisuje politykę bezpieczeństwa i cele do osiągnięcia, opisuje wymagania SMS, procesy i procedury, odpowiedzialność ogólną, wskazuje odpowiedzialnych za zadania i uprawnionych do podejmowania działań i procedur oraz rezultaty wynikające z SMS. Także jako część dokumentacji SMS, [organizacja] opracowuje i prowadzi podręcznik systemu zarządzania bezpieczeństwem (SMSM), aby pokazać swoje podejście do zarządzania bezpieczeństwem w całej organizacji.

## 2. ZARZĄDZANIE RYZYKIEM

### 2.1 Identyfikacja zagrożeń

[Organizacja] opracowuje i prowadzi formalny proces, który zapewnia, że zagrożenia związane z działalnością operacyjną zostały zidentyfikowane.
Identyfikacja zagrożeń opiera się na połączeniu metod reaktywnych, proaktywnych i prognozowaniu w oparciu o zebrane dane.

### 2.2 Ocena ryzyka i jego minimalizowanie

[Organizacja] opracowuje i prowadzi formalny proces analizy, oceny i kontroli ryzyka podczas działalności operacyjnej [organizacji].

## 3. ZAPEWNIENIE BEZPIECZEŃSTWA

### 3.1 Monitorowania poziomu bezpieczeństwa i pomiar

[Organizacja] opracowuje i utrzymuje środki w celu sprawdzenia poziomu bezpieczeństwa w organizacji i sprawdzenia skuteczności kontroli ryzyka. Poziom bezpieczeństwa w organizacji jest weryfikowany w odniesieniu do wskaźników bezpieczeństwa i do wcześniej założonych celów związanych z poziomem bezpieczeństwa wyznaczonych w SMS.

### 3.2 Zarządzanie zmianami

[Organizacja] opracowuje i prowadzi formalny proces: aby zidentyfikować zmiany w organizacji, które mogą mieć wpływ na procesy i działania operacyjne; aby przed wprowadzeniem zmian dokładnie je opisać w celu zachowania poziomu bezpieczeństwa oraz aby wyeliminować lub zmienić procesy kontroli ryzyka, które nie są już potrzebne lub skuteczne ze względu na zmiany w środowisku operacyjnym.

### 3.3 Ciągłe doskonalenie systemu zarządzania

[Organizacja] opracowuje i prowadzi formalny proces do identyfikacji przyczyn braków w wydajności SMS, ustali wpływ tych braków na wykonywanie operacji, i wyeliminuje lub zmniejszy takie przyczyny.

## 4. PROPAGOWANIE BEZPIECZEŃSTWA

### 4.1 Szkolenie i edukacja

[Organizacja] opracowuje i prowadzi program szkolenia w zakresie bezpieczeństwa, który zapewnia, że personel jest przeszkolony i posiada właściwe kompetencje, aby wypełniać obowiązki związane z SMS. Zakres szkolenia w zakresie bezpieczeństwa powinien być dostosowany do indywidualnych działań w ramach SMS.

### 4.2 Komunikacja w zakresie bezpieczeństwa.

[Organizacja] opracowuje i utrzymuje formalne środki komunikacji w zakresie bezpieczeństwa, które zapewniają, że personel jest w pełni świadomy SMS, informacje krytyczne dla bezpieczeństwa są przekazywane, i które to środki komunikacji zapewniają wyjaśnienie wszystkim dlaczego poszczególne działania na rzecz bezpieczeństwa są podejmowane, a także dlaczego procedury bezpieczeństwa są wprowadzane lub zmienione.

## Dodatek 2 do Rozdziału 8

# PRZYKŁADOWY OPIS STANOWISKA PRACY DYREKTORA DS. BEZPIECZEŃSTWA

### 1. OPIS OGÓLNY

Dyrektor ds. bezpieczeństwa jest odpowiedzialny za dostarczenie wytycznych i zaleceń w zakresie planowania, realizacji i eksploatacji systemu zarządzania bezpieczeństwem (SMS) w organizacji.

### 2. KLUCZOWE ROLE

**Rzecznik Bezpieczeństwa**

- Wykazuje doskonałą postawę i nastawienie promujące zachowanie bezpieczeństwa, przestrzega praktyk regulacyjnych i przepisów, rozpoznaje i zgłasza zagrożenia oraz sprzyja zgłaszaniu nieprawidłowości przez innych.

**Lider**

- Poprzez efektywne przywództwo, kształtuje i promuje kulturę organizacyjną, która wspiera zasady bezpieczeństwa.

**Informator**

- Działa jako źródło i transmiter informacji w kwestii bezpieczeństwa do wiadomości zarządu oraz przekazuje zagadnienia bezpieczeństwa pracownikom, kontrahentom i innym zainteresowanym stronom.
- Jasno wyraża informacje dotyczące zagadnień bezpieczeństwa w organizacji.

**Developer**

- Pomaga w ciągłym doskonaleniu systemów identyfikacji zagrożeń i oceny ryzyka oraz organizacji SMS.

**Towarzyski**

- Buduje i utrzymuje doskonałą współpracę z grupą działania na rzecz bezpieczeństwa i w biurze/komitecie/departamencie związanym z bezpieczeństwem.

**Ambasador**

- Reprezentuje organizację przed organizacjami rządowymi, międzynarodowymi i innymi stowarzyszeniami (np. ICAO, IATA, CAA, AIB itp.).

**Analityk**

- Analizuje zebrane dane techniczne pod kątem trendów związanych z zagrożeniami, zdarzeniami i okolicznościami mającymi wpływ na bezpieczeństwo.

**Kierujący procesami**

- Skutecznie wykorzystuje dostępne procesy i procedury do podziału ról i obowiązków w organizacji.
- Bada dostępne możliwości w celu zwiększenia efektywności procesów.
- Mierzy skuteczność procedur i działań oraz dąży do ciągłego doskonalenia jakości procesów.

### 3. OBOWIĄZKI

3.1 Stanowisko wymaga umiejętności radzenia sobie ze zmieniającymi się okolicznościami i sytuacjami, wymagany jest tylko niewielki nadzór. Dyrektor ds. bezpieczeństwa działa niezależnie od innych menedżerów w organizacji.

3.2 Dyrektor ds. bezpieczeństwa jest odpowiedzialny za dostarczanie informacji i porad dla kierownictwa wyższego szczebla oraz innych osób odpowiedzialnych w sprawach dotyczących bezpieczeństwa operacji. Wymagane jest poczucie taktu, dyplomacji i wysoki stopień integralności z innymi.

3.3 Praca wymaga elastyczności, ponieważ zadania mogą wymagać działań w krótkim czasie lub nawet bez uprzedzenia i poza normalnymi godzinami pracy.

### 4. CHARAKTER I ZAKRES

Dyrektor ds. bezpieczeństwa musi współdziałać z personelem operacyjnym i kierownikami działów w całej organizacji. Dyrektor ds. bezpieczeństwa powinien również dbać o pozytywne relacje z organami regulacyjnymi, zewnętrznymi agencjami i dostawcami usług. W razie potrzeby inne kontakty zostaną ustalone na poziomie roboczym.

### 5. KWALIFIKACJE

Kwalifikacje obejmują:

a) szeroką wiedzę i doświadczenie operacyjne w poszczególnych działach organizacji (np. szkolenia z zarządzania, eksploatacji statków powietrznych, zarządzania ruchem lotniczym, funkcjonowania i utrzymywania lotniska);

b) dobrą znajomość zasad zarządzania bezpieczeństwem i praktyk SMS;

c) wysoką umiejętność komunikacji;

d) dobrze rozwinięte umiejętności interpersonalne;

e) umiejętność obsługi komputera;

f) zdolność do komunikacji na wszystkich szczeblach, zarówno wewnątrz, jak i na zewnątrz organizacji;

g) zdolności organizacyjne;

h) umiejętność pracy bez nadzoru;

i) dobre umiejętności analityczne;

j) umiejętności przywódcze i budzące zaufanie podejście;

k) wzbudzanie szacunku ze strony rówieśników i zarządzających.

### 6. KOMPETENCJE

6.1 W odniesieniu do kwestii bezpieczeństwa, Dyrektor ds. bezpieczeństwa ma bezpośredni dostęp do najwyższego zwierzchnika i kierowników wyższego i średniego szczebla zarządzania.

6.2 Dyrektor ds. bezpieczeństwa jest uprawniony do przeprowadzania audytów bezpieczeństwa, badań i kontroli wszelkich aspektów wykonywanych operacji.

6.3 Dyrektor ds. bezpieczeństwa posiada uprawnienia do prowadzenia wewnętrznych dochodzeń w przypadku zdarzeń i okoliczności mających wpływ na bezpieczeństwo, zgodnie z procedurami określonymi w Podręczniku Zarządzania Systemem Bezpieczeństwa (SMSM) organizacji.

---

# Rozdział 9

# DZIAŁANIE SMS

## 9.1 CEL I ZAWARTOŚĆ

Niniejszy rozdział opisuje wymagania związane z funkcjonowaniem SMS, korzystając ze schematu SMS ICAO jako odniesienia. Pierwszy jego element został omówiony w rozdziale 8. Niniejszy rozdział omawia pozostałe trzy elementy schematu. Rozdział ten omawia poniższe zagadnienia:

a) Zarządzanie ryzykiem — Uwagi ogólne;

b) Identyfikacja zagrożeń;

c) Ocena ryzyka i jego łagodzenie;

d) Zapewnienie bezpieczeństwa – Uwagi ogólne;

e) Monitorowanie i ocena poziomu bezpieczeństwa;

f) Zabezpieczanie źródeł informacji o bezpieczeństwie;

g) Zarządzanie zmianami;

h) Ciągłe usprawnianie SMS;

i) Współzależność pomiędzy zarządzaniem ryzykiem bezpieczeństwa (SRM) a zapewnieniem bezpieczeństwa (SA);

j) Promowanie bezpieczeństwa — Szkolenie i edukacja;

k) Promowanie bezpieczeństwa — Informowanie o bezpieczeństwie.

## 9.2 ZARZĄDZANIE RYZYKIEM — UWAGI OGÓLNE

9.2.1 Organizacja zarządza bezpieczeństwem poprzez swój proces zarządzania ryzykiem, zapewniając, że zagrożenie ryzykami bezpieczeństwa będące konsekwencją zagrożeń występujących w krytycznych czynnościach związanych z dostarczaniem usług jest utrzymywane na poziomie najniższym z możliwych (ALARP). To pojęcie znane jest jako zarządzanie ryzykiem i obejmuje dwie, absolutnie różne dziedziny: identyfikację zagrożeń oraz ocenę ryzyka bezpieczeństwa i jego łagodzenie.

9.2.2 Zarządzanie ryzykiem bezpieczeństwa oparte jest na zaprojektowanym systemie, w którym odpowiednie zabezpieczenia przed ryzykiem bezpieczeństwa eliminują lub łagodzą konsekwencje zakładanych zagrożeń osadzone są w systemie. Niezależnie czy „system”, o którym mowa, jest systemem fizycznym, takim jak statek powietrzny, czy systemem organizacyjnym, takim jak linia lotnicza, lotnisko czy dostawca usług ruchu lotniczego to stwierdzenie jest prawdziwe. W odniesieniu do niniejszego podręcznika, ten ostatni – system organizacyjny – jest „systemem”, który jest omawiany częściej. Organizacja jest systemem składającym się ze struktur, procesów i procedur, jak również personelu, sprzętu i obiektów, które są potrzebne do zrealizowania misji systemu.

### 9.3 IDENTYFIKACJA ZAGROŻEŃ

9.3.1 Zarządzanie ryzkiem rozpoczyna się od opisu funkcji systemu, który stanowi podstawę do identyfikacji zagrożeń (patrz rozdział 7). W opisie systemu, jego elementy i ich współdziałanie ze środowiskiem operacyjnym systemu, są analizowane pod kątem występowania zagrożeń, jak również dla zidentyfikowania już istniejących w systemie zabezpieczeń od ryzyka lub jego braku (proces zwany analizą luk w systemie, omówiony wcześniej w rozdziale 7). Ryzyka bezpieczeństwa analizowane są w kontekście opisanego systemu, a ich potencjalne niszczące/destrukcyjne konsekwencje zidentyfikowane i przeanalizowane w odniesieniu do ryzyk bezpieczeństwa (prawdopodobieństwo i dotkliwe skutki niszczącego potencjału zidentyfikowanych konsekwencji omówiono w rozdziale 5). Tam, gdzie ryzyka bezpieczeństwa, będące konsekwencją zagrożeń są ocenione jako za wysokie do zaakceptowania, należy wprowadzić do systemu dodatkowe zabezpieczenia monitorujące ryzyko bezpieczeństwa. Tak więc, zasadniczym elementem zarządzania bezpieczeństwem jest ocena projektu systemu i weryfikacja czy wystarczająco kontroluje on skutki zagrożeń.

9.3.2 Tak więc pierwszym krokiem w formalnym procesie zbierania, rejestrowania, reagowania i przygotowywania informacji o zagrożeniach i ryzykach bezpieczeństwa dla operacji jest identyfikacja zagrożeń. W prawidłowo uruchomionym SMS, źródła identyfikacji zagrożeń muszą uwzględniać trzy metody omówione w rozdziale 3: metoda reaktywna, proaktywna i metoda przewidywania. Sam proces identyfikacji zagrożeń omówiony jest w rozdziale 4.

9.3.3 Strukturalne podejście do identyfikacji zagrożeń zapewnia, na ile jest to możliwe, że zidentyfikowano wszystkie zagrożenia w środowisku operacyjnym systemu. Odpowiednie techniki gwarantujące takie strukturalne podejście mogą uwzględniać:

a) ***Listy kontrolne.*** Zapoznanie się z doświadczeniem i dostępnymi danymi podobnych systemów i opracowanie listy kontrolnej zagrożeń. Potencjalnie niebezpieczne obszary wymagać będą dodatkowej oceny.

b) ***Przegląd grupowy.*** Można wykorzystać sesje grupowe dla przeanalizowania listy kontrolnej, szerszego przedyskutowania zagrożeń albo dla przeprowadzenia szczegółowej analizy.

9.3.4 Sesje poświęcone identyfikacji zagrożeń wymagają udziału doświadczonego personelu operacyjnego i technicznego, i prowadzone są zazwyczaj w formie kontrolowanej dyskusji grupowej. Taką sesję grupową powinna prowadzić osoba, która zna techniki prowadzenia „burzy mózgów". Rolę taką mógłby spełniać Dyrektor ds. bezpieczeństwa, jeżeli został wyznaczony. Wykorzystanie sesji grupowej jest tutaj omawiane w kontekście identyfikacji zagrożeń, ale ta sama grupa również mogłaby omówić prawdopodobieństwo i dotkliwość ryzyk bezpieczeństwa wynikających z konsekwencji zidentyfikowanych przez siebie zagrożeń.

9.3.5 Analiza zagrożeń powinna rozważać wszystkie możliwości, od najmniej do najbardziej prawdopodobnych. Należy również uwzględnić warunki dla „najgorszego przypadku", ale równie ważnym jest, aby zagrożenia włączane do końcowej analizy były „wiarygodne". Często trudno jest określić granicę pomiędzy najgorszym, ale wiarygodnym przypadkiem, a takim, który jest tak uzależniony od zbiegu okoliczności, że nie powinien być brany pod uwagę. Można wykorzystać poniższe definicje jako pomoc przy podejmowaniu takich decyzji:

a) ***Najgorszy przypadek.*** Najbardziej niesprzyjające warunki jakich można się spodziewać, np. niezwykle duży ruch lotniczy i ekstremalna zmiana pogody.

b) ***Przypadek wiarygodny.*** Zakłada, że wystąpienie zakładanej kombinacji ekstremalnych warunków w cyklu żywotności operacyjnej systemu nie jest niedorzeczne.

9.3.6 Wszystkim zidentyfikowanym zagrożeniom należy przypisać numer i odnotować w rejestrze zagrożeń (przykłady rejestrów zagrożeń można znaleźć w dodatku do rozdziału 5). Rejestr zagrożeń musi zawierać opis każdego zagrożenia, jego konsekwencje, określone prawdopodobieństwo i dotkliwość konsekwencji ryzyk bezpieczeństwa oraz wymagane zabezpieczenia, zazwyczaj działania łagodzące. Rejestr zagrożeń należy uaktualniać wraz z identyfikacją nowych zagrożeń i propozycją wprowadzenia dodatkowych zabezpieczeń od ryzyka bezpieczeństwa (tzn. dalszych działań łagodzących).

### 9.4 OCENA RYZYKA I JEGO ŁAGODZENIE

9.4.1 Po zidentyfikowaniu zagrożeń należy ocenić ryzyka bezpieczeństwa, ich ewentualne konsekwencje (rozdział 5). Ocena ryzyk bezpieczeństwa jest analizą ryzyka bezpieczeństwa skutków zagrożeń, które zostały uznane jako zagrażające zdolnościom organizacji. Do oceny ryzyka bezpieczeństwa stosuje się konwencjonalny podział ryzyka na dwa elementy – prawdopodobieństwo wystąpienia niszczącego zdarzenia lub jego dotkliwość, jeżeli takie zdarzenie wystąpi. Podejmowanie decyzji o ryzyku bezpieczeństwa i jej akceptacja jest określana w oparciu o tabelę tolerancji ryzyka. Poza tabelą, wymagany jest również rozsądek. Definicja i ostateczny projekt konstrukcji tabeli, powinien być pozostawiony organizacji świadczącej usługę, ale uzgodniony z organizacją nadzorującą celem dopilnowania, czy narzędzia służące podejmowaniu decyzji o bezpieczeństwie w każdej organizacji, są odpowiednie dla jej operacji, środowiska operacyjnego i uwzględniają szeroką dywersyfikację w tym obszarze.

9.4.2 Po dokonaniu, zgodnie z powyższym opisem, oceny ryzyk bezpieczeństwa, należy podjąć działania celem ich usunięcia lub/i złagodzenia do poziomu ALARP. Znane to jest jako łagodzenie ryzyka. Należy opracować i wdrożyć zabezpieczenia przed ryzykiem bezpieczeństwa. Może to być w formie nowych lub zmienionych procedur, nowych, nadzorowanych zabezpieczeń zmian w szkoleniu, dodatkowego lub zmodyfikowanego wyposażenia lub dowolnych innych alternatywnych działań służących usuwaniu/łagodzeniu. Prawie na pewno, alternatywy te będą związane z rozwinięciem lub ponownym uruchomieniem trzech tradycyjnych lotniczych systemów obronnych (technologia, szkolenie i przepisy) lub ich kombinacji. Po zaprojektowaniu zabezpieczeń przed ryzykiem bezpieczeństwa, ale przed uruchomieniem systemu, należy dokonać oceny i sprawdzić czy wprowadzone zabezpieczenia nie stwarzają nowych zagrożeń dla systemu.

9.4.3 W tym momencie system jest gotowy do operacyjnego rozwinięcia/ponownego uruchomienia, zakładając, że zabezpieczenia przed ryzykiem bezpieczeństwa są uznane za dopuszczalne. Kolejny element SMS, zapewnienie bezpieczeństwa, wykorzystuje audytowanie, analizy, oceny i podobne techniki, równolegle z tymi wykorzystywanymi przez system zarządzania jakością. Techniki te stosowane są do monitorowania zabezpieczeń przed ryzykiem bezpieczeństwa, celem zapewnienia, że wdrażane są one nadal zgodnie z projektem i nadal są skuteczne w dynamicznym środowisku operacyjnym.

### 9.5 ZAPEWNIENIE BEZPIECZEŃSTWA — UWAGI OGÓLNE

9.5.1 Aby zamknąć pełen cykl zarządzania bezpieczeństwem, zarządzanie ryzykiem bezpieczeństwa wymaga informacji, w jaki sposób realizowane są założenia bezpieczeństwa. Poprzez monitorowanie i otrzymywanie informacji, można ocenić jak funkcjonuje SMS i wszelkie wprowadzane do niego zmiany. Ponadto zapewnienie bezpieczeństwa dostarcza interesariuszom wskazań co do poziomu bezpieczeństwa systemu.

9.5.2 Zapewnienie można w prosty sposób zdefiniować jako “coś czemu można zaufać”. Proces zarządzania ryzykiem w SMS zaczyna się, gdy organizacja dobrze zrozumie swoje procesy operacyjne i środowisko, w którym działa, przechodzi przez identyfikację zagrożenia, ocenę ryzyka i jego łagodzenia i osiąga szczyt w momencie opracowania i wdrożenia odpowiednich zabezpieczeń przed ryzykiem bezpieczeństwa. Po opracowaniu zabezpieczeń przed ryzykiem bezpieczeństwa stanowiącego konsekwencję zagrożeń oraz uruchomienie i uznanie ich jako zdolnych do kontrolowania ryzyka, to zapewnienie bezpieczeństwa przejmuje zarządzanie ryzykiem.

9.5.3 Po opracowaniu i wdrożeniu zabezpieczenia przed ryzykiem bezpieczeństwa, organizacja staje się odpowiedzialna za zapewnienie, że zabezpieczenia te pozostają na miejscu i działają zgodnie z zamierzeniami. Zgodnie z powyższą definicją „zapewnienia”, składa się ona z procesów i czynności podejmowanych przez organizację celem zapewnienia wiarygodności co do działania i skuteczności zabezpieczeń. Organizacja na bieżąco musi monitorować swoje operacje i środowisko, aby zapewniać, że rozpoznaje zachodzące w środowisku operacyjnym zmiany, które mogłyby wskazywać na pojawienie się nowych, nie złagodzonych zagrożeń oraz wskazywać na degradację w procesach operacyjnych, obiektach, stanie wyposażenia lub w pracy człowieka. Mogłoby to obniżyć skuteczność istniejących zabezpieczeń od skutków ryzyka bezpieczeństwa. Wskazywałoby na konieczność powrotu do procesu zarządzania ryzykiem celem dokonania przeglądu i, jeżeli konieczne, dokonania zmian w istniejących zabezpieczeniach przed ryzykiem bezpieczeństwa lub opracowania nowych.

9.5.4 Proces ciągłego sprawdzania, analizowania i przeglądania zabezpieczeń musi odbywać się w trakcie codziennych operacji systemu. Proces zapewnienia bezpieczeństwa odzwierciedla proces zapewnienia jakości z jego wymaganiami dotyczącymi analiz, dokumentacji, audytowania i oceny kierownictwa, co do skuteczności zabezpieczeń ryzyka bezpieczeństwa. Różnica to nacisk na potwierdzenie w zapewnieniu bezpieczeństwa, że zabezpieczenia od ryzyka bezpieczeństwa są na swoim miejscu, są sprawdzane i pozostają skuteczne. W zapewnieniu jakości nacisk tradycyjnie kładziony jest na zadowolenie klienta, które, chyba że realizowane z odpowiedniej perspektywy, może lub nie musi być całkowicie zgodne z akceptacją bezpieczeństwa. Krótka dyskusja poniżej.

9.5.5 W lotnictwie zapewnienie jakości jest tradycyjne, związane z obsługą i produkcją, a rzadziej stosowane w operacjach związanych z lotem, z wyjątkiem ograniczonego zastosowania w szkoleniu i sprawdzaniu. Niektóre wcześniejsze przepisy żądały programów zapewnienia jakości, aczkolwiek wymagania te nie były całościowe ani dobrze zdefiniowane dla wszystkich funkcji w organizacji. Faktem pozostaje jednak to, że zapewnienie jakości jest pojęciem znanym, aczkolwiek często powiązanym z zadowoleniem klienta i osiągnięciami o założeniach handlowych niż związanych z bezpieczeństwem. Pomimo to, techniki gwarantujące zrealizowanie celów handlowych organizacji i stosowane w procesach zapewniania jakości mają również swoje zastosowanie w procesach zapewnienia bezpieczeństwa. Aby móc stosować te techniki w procesach zapewniania bezpieczeństwa, organizacja musi być ostrożna w ustanawianiu i ocenie celów w odniesieniu do bezpieczeństwa.

9.5.6 Najważniejsze dla organizacji jest opracowanie i wdrożenie wszystkich procesów operacyjnych w taki sposób, aby w oparciu o solidne stosowanie zasad zarządzania ryzykiem, włączyć do niego zabezpieczenia przed ryzykiem bezpieczeństwa, wraz z gwarancją ich skuteczności. Wybór nazwy przez organizację –„jakość" czy „bezpieczeństwo" – dla procesów zapewnienia ma mniejsze znaczenie pod warunkiem, że SMS koncentruje się na bezpieczeństwie.

9.5.7 Rozdział 6 omawia podejścia oparte na wynikach zarządzania bezpieczeństwem. Jeden z aspektów, który można przeoczyć przy zapewnianiu wyników, chyba że zachowana jest odpowiednia perspektywa, to uwzględnienie zapewnienia zgodności prawnej. Rozdział 6 wprowadza pojęcie przepisów jako zabezpieczenia przed ryzykiem. Same w sobie, przepisy stanowią integralną część procesu zarządzania ryzykiem. W prawidłowo uruchomionym SMS nie powinien występować żaden konflikt pomiędzy zapewnieniem ryzyka bezpieczeństwa a zapewnieniem zgodności z przepisami. Przepisy powinny stanowić część projektu systemu, a zgodność prawna i zarządzanie ryzykiem są fragmentami tej samej całości. Nadal oczekuje się przestrzegania przepisów określających to, co powinno znaleźć się w zakresie zapewnienie bezpieczeństwa, jako czynność ukierunkowana na „dawanie wiary" w funkcjonowanie SMS.

9.5.8 W podsumowaniu, kierownictwo, aby utrzymać rentowność organizacji równolegle z utrzymywaniem bezpieczeństwa operacji, musi zapewnić równowagę pomiędzy zadawalającym bezpieczeństwem a zadowolonym klientem. Podczas, gdy połączenie założeń SMS i QMS może przyczynić się do oszczędności zasobów, to prawdopodobieństwo niedopasowania założeń dotyczących zadawalającego bezpieczeństwa i zadowolonego klienta oznacza, że nie są one automatycznie zamienne ani nawet równe. Zapewnienie połączenia takiego typu leży w gestii kierownictwa organizacji. Ocena funkcjonowania systemu i weryfikacja czy możliwości systemu nadal kontrolują ryzyko w aktualnym środowisku operacyjnym, z punktu widzenia zarządzania bezpieczeństwem pozostaje podstawowym tematem zainteresowania.

9.5.9 I na koniec, czynności związane z zapewnieniem bezpieczeństwa powinny uwzględniać procedury zapewniające opracowanie działań naprawczych jako odpowiedź na wnioski pokontrolne, badania, audyty, oceny itd. i weryfikację skutecznego, terminowego wdrożenia. Organizacyjnie, odpowiedzialność za przygotowanie i wdrożenie działań naprawczych powinna znaleźć sie w gestii departamentów operacyjnych wymienionych we wnioskach. Jeżeli pojawiają się nowe zagrożenia, należy uruchomić proces zarządzania ryzykiem w celu określenia czy zachodzi konieczność opracowania nowych zabezpieczeń przed ryzykiem bezpieczeństwa.

### 9.6 MONITOROWANIE I OCENA POZIOMU BEZPIECZEŃSTWA

9.6.1 Podstawowym zadaniem zapewnienia bezpieczeństwa jest kontrola. Jest to realizowane poprzez monitorowanie i określenie poziomu bezpieczeństwa. Proces ten, weryfikuje bezpieczeństwo w odniesieniu do polityki bezpieczeństwa i zatwierdzonych założeń. Kontrola zapewnienia bezpieczeństwa jest realizowana przez monitorowanie i ocenę rezultatów/wyników czynności podejmowanych przez personel w celu zrealizowania usługi przez organizację.

9.6.2 Międzynarodowa norma zarządzania jakością, ISO-9000, przedstawia następującą definicję procesu: „…powiązany ze sobą komplet czynności, które przekształcają wkład w wyniki". Nacisk na „czynności" jako zasadnicze „rzeczy, które robią ludzie" jest powodem, dla którego w dyskusjach na temat bezpieczeństwa i zarządzania bezpieczeństwem, zawartych w rozdziale 2 i 3, kładziony jest nacisk na błąd człowieka i warunki pracy, a następnie przeniesiony on jest na zarządzanie ryzykiem. Te warunki stanowią źródło większości zagrożeń i na tych warunkach trzeba skoncentrować większość zabezpieczeń przed ryzykiem bezpieczeństwa. Tak więc, większość czynności zapewniających bezpieczeństwo, realizowanych pod szyldem monitorowanie i określanie poziomu bezpieczeństwa, koncentruje się na warunkach pracy, które mają wpływ na sposób wykonywania koniecznych czynności w celu zrealizowania usługi. Z tego też powodu model SHEL – model systemów wspomagających wykonanie czynności operacyjnych składających się na realizację usług – proponowany jest jako wskazówka do opisu systemu i analizy luk w systemie.

9.6.3 Poniżej znajduje się wykaz rodzajowych zagadnień i obszarów, które należy rozważyć, aby „zapewnić bezpieczeństwo" poprzez jego monitorowanie i określenie poziomu bezpieczeństwa:

a) ***Odpowiedzialność.*** Kto jest odpowiedzialny za zarządzanie czynnościami operacyjnymi (planowanie, organizowanie, kierowanie, kontrolowanie) i ich pełne wykonanie.

b) ***Władza.*** Kto może kierować, kontrolować lub zmieniać procedury, a kto nie oraz kto może podejmować kluczowe decyzje takie jak decyzja o akceptacji ryzyka.

c) ***Procedury.*** Wyszczególnione sposoby określające w jaki sposób wykonywać czynności operacyjne i tłumaczące w jaki sposób zamienić „co" (założenia) na „jak" (czynności praktyczne).

d) ***Zabezpieczenia***. Elementy systemu, włącznie z oprzyrządowaniem, oprogramowaniem, specjalnymi procedurami lub etapami proceduralnymi oraz praktyki nadzoru tak opracowane, aby utrzymywać czynności operacyjne na właściwej drodze.

e) ***Interfejs.*** Analiza takich rzeczy jak relacje służbowe/kompetencje departamentów, drogi komunikowania się między pracownikami, zgodność procedur i wyraźne rozpisanie obowiązków pomiędzy organizacje, stanowiska pracy i pracowników.

f) ***Ocena procesu.*** Sposoby przekazywania informacji zwrotnej odpowiedzialnym stronom, że wymagane działania są podejmowane oraz, że osiągane są założone rezultaty.

9.6.4 Informacje o monitorowaniu i poziomie bezpieczeństwa pochodzą z różnych źródeł, włącznie z oficjalnym audytowaniem i oceną, badaniem zdarzeń związanych z bezpieczeństwem, ciągłym monitorowaniem codziennych czynności związanych z realizacją usług oraz wkładem pracowników poprzez systemy raportowania o zagrożeniu. Wszystkie te źródła informacji mogą, w jakimś stopniu, występować w każdej organizacji.. Jednak wykaz pożądanych źródeł lub określenie „jak powinny one wyglądać" należy pozostawić na poziomie operacyjnym, pozwalając organizacjom dopasowanie ich do swojego zakresu i skali odpowiedniej dla wielkości i typu organizacji. Źródła informacji dla monitorowania i określania poziomu bezpieczeństwa obejmują:

a) zgłaszanie zagrożeń;

b) analizy bezpieczeństwa;

c) przeglądy bezpieczeństwa;

d) audyty;

e) badania bezpieczeństwa;

f) wewnętrzne badania dotyczące bezpieczeństwa.

9.6.5 Zgłaszanie zagrożeń i systemy zgłaszania zagrożeń stanowią podstawowe elementy identyfikacji zagrożenia. Nikt lepiej, aniżeli personel operacyjny, nie wie jak działa system. Organizacja, która chce wiedzieć jak funkcjonuje codziennie, w przeciwieństwie do sposobu w jaki powinna funkcjonować zgodnie „z podręcznikiem", powinna o to pytać personel operacyjny, stąd takie znaczenie systemów zgłaszania. Istnieją trzy systemy zgłaszania:

a) obowiązkowe systemy zgłaszania;

b) dobrowolne systemy zgłaszania;

c) poufne systemy zgłaszania.

9.6.6 ***W obowiązkowych systemach zgłaszania***, osoby są zobowiązane do zgłaszania pewnych typów zdarzeń lub zagrożeń. To wymusza opracowanie szczegółowych przepisów określających kto ma zgłaszać i co ma być zgłaszane. Ponieważ systemy obowiązkowe, dotyczą głównie zagadnień związanych z „oprzyrządowaniem", mają tendencję do zbierania większej ilości informacji na temat awarii technicznych niż innych aspektów działalności operacyjnej. Aby tego uniknąć, wprowadzono dobrowolny system zgłaszania, którego celem jest pozyskiwanie większej ilości informacji o pozostałych aspektach działalności operacyjnej.

9.6.7 ***W dobrowolnych systemach zgłaszania,*** zgłaszający, bez żadnego prawnego lub administracyjnego obowiązku, dobrowolnie zgłasza zdarzenia lub informacje o zagrożeniu. W tych systemach, regulacyjne agencje i/lub organizacje mogą zachęcać do takich zachowań. Np. można zaniechać podejmowania działań egzekucyjnych wobec zgłoszonych zdarzeń, za którymi stoją błędy lub niezamierzone naruszenia przepisów. Zgłoszona informacja nie powinna być wykorzystana przeciwko zgłaszającemu, tzn. takie systemy nie powinny karać, natomiast zapewniać ochronę źródłom informacji, aby zachęcać do zgłaszania takich informacji.

9.6.8 ***Celem poufnych systemów zgłaszania*** jest ochrona tożsamości zgłaszającego. Jest to jeden ze sposobów gwarantujący, że w dobrowolnych systemach zgłaszania nie ma kar. Poufność uzyskuje się zazwyczaj przez likwidowanie tożsamości, tak, że wszelkie informacje związane z tożsamością zgłaszającego znane są tylko „strażnikom", aby móc kontrolować co się dalej dzieje lub „uzupełnienia pustych miejsc" w zgłoszonym zdarzeniu(-ach). Systemy poufnego zgłaszania zdarzeń ułatwiają ujawnienie zagrożeń prowadzących do błędu człowieka, bez obawy bycia ukaranym oraz umożliwiają szersze pozyskiwanie informacji o zagrożeniach.

9.6.9 Podczas gdy podstawowe procesy tkwiące u podstaw systemów zgłaszania są znormalizowane, faktycznie stosowane sposoby mogą różnić się między Państwami i organizacjami. Aby zapewnić skuteczność takich systemów należy również podkreślić, że personel operacyjny jest niechętny procesowi zgłaszania. To stwierdzenie ma zastosowanie do wszystkich form zgłaszania, a w szczególności tam, gdzie wchodzi w grę zgłaszanie własnych błędów. Są powody takiej niechęci: obawa przed odwetem, oskarżeniem samego siebie i wstydem. To tylko trzy najważniejsze z nich. Zasadnicza strategia podejścia do niechęci zgłaszania to zapewnienia poufności i edukacja na temat zgłaszania zagadnień dot. bezpieczeństwa w systemach identyfikacji zagrożeń, omówiona w rozdziale 2, i ochrona źródeł informacji o bezpieczeństwie (omówione w sekcji 9.7). Typowe właściwości skutecznych systemów zgłaszania informacji dot. bezpieczeństwa uwzględniają:

a) zgłoszenia są łatwe do opracowania/wypełnienia;

b) w wyniku zgłoszeń nie podejmowane są żadne działania dyscyplinarne;

c) zgłoszenia są poufne;

d) informacja zwrotna jest szybka, dostępna i pouczająca.

9.6.10 ***Badanie bezpieczeństwa*** to bardzo rozległe analizy obejmujące szeroko rozumiane zagadnienia z nim związane. Niektóre, rozpowszechnione zagadnienia dot. bezpieczeństwa można najlepiej zrozumieć poprzez ich dogłębne zbadanie w możliwie najszerszym kontekście. Organizacja może mieć problem związany z bezpieczeństwem o charakterze światowym, który był już omawiany w sektorze lub na arenie międzynarodowej. Np., linia lotnicza zauważa wzrost zdarzeń występujących podczas podejścia lub lądowania (niestabilne podejścia, twarde lądowania, lądowania z nadmierną prędkością itd.). Przemysł na świecie zaniepokoił się częstotliwością i drastycznością wypadków podczas podejścia i lądowania (ALA) w związku z czym podjęto intensywne badania nad tym zagadnieniem, wypracowano wiele zaleceń związanych z bezpieczeństwem

i wdrożono działania na skalę światową, aby obniżyć liczbę takich zdarzeń podczas krytycznych faz podejścia i lądowania. Zatem zainteresowana linia lotnicza może w tych zaleceniach i badaniach na skalę światową, znaleźć przekonujące argumenty dla własnej, wewnętrznej analizy bezpieczeństwa. Argumenty takie są potrzebne, aby wprowadzić poważne zmiany na dużą skalę wymagające znaczących danych, odpowiednich analiz i skutecznej komunikacji. Argumenty dotyczące bezpieczeństwa oparte na odosobnionych zdarzeniach i informacji o charakterze anegdoty mogą nie wystarczać. Ze względu na swój charakter, badanie bezpieczeństwa jest odpowiedniejsze dla określenia niedoborów w systemie bezpieczeństwa niż dla identyfikowania specyficznych, pojedynczych zagrożeń.

9.6.11 ***Przeglądy bezpieczeństwa*** wykonywane są w trakcie wprowadzania i uruchamiania nowych technologii, podczas zmiany lub wdrażania procedur lub w sytuacjach strukturalnych zmian w operacjach. Przeglądy bezpieczeństwa stanowią podstawowy element zarządzania zmianami, omawianymi w sekcji 9.8. Mają one wyraźnie zdefiniowane założenie powiązane z rozważaną zmianą. Np., lotnisko rozważa wdrożenie sprzętu wykrywania zmian w nawierzchni lotniska (ASDE). Tak więc założeniem przeglądu bezpieczeństwa byłaby ocena ryzyka związanego z wdrożeniem ASDE na lotnisku XYZ poprzez ocenę stosowności i skuteczności czynności

zarządzania bezpieczeństwem powiązanym z projektem. Przeglądy bezpieczeństwa wykonywane są przez Safety Action Groups (SAG), które sprawdzają skuteczność działania następujących czynności zarządzania bezpieczeństwem powiązanych z proponowanymi zmianami:

a) identyfikacja zagrożenia i ocena/łagodzenie ryzyka;

b) ocena poziomu bezpieczeństwa;

c) odpowiedzialność kierownictwa;

d) umiejętności operacyjne pracowników;

e) systemy techniczne;

f) operacje nienormalne.

9.6.12 Po dokonaniu przeglądu każdej czynności zarządzania bezpieczeństwem w powiązaniu z proponowanymi zmianami SAG opracowuje wykaz zagrożeń oraz ocenę stosowności i skuteczności łagodzenia zagrożenia. Łagodzenie będzie skuteczne, jeżeli w normalnych warunkach operacyjnych konsekwentnie zarządza ryzykiem w celu zmniejszenia ryzyk bezpieczeństwa dla ALARP. SAG również proponuje kolejność reakcji/łagodzeń, poprzez przyznanie ważności i pilności każdemu zagrożeniu. Tak więc, przeglądy bezpieczeństwa zapewniają utrzymanie odpowiedniego poziomu bezpieczeństwa w okresach wprowadzania zmian, poprzez przygotowanie harmonogramu prowadzącego do bezpiecznej i skutecznej zmiany.

9.6.13 ***Audyty*** koncentrują się na integralności SMS organizacji i okresowo oceniają status zabezpieczeń przed ryzykiem. Podobnie jak z innymi wymaganiami, wymagania audytowe pozostawione są na poziomie funkcjonalnym, pozwalając na szeroki zakres złożoności, współmierny ze złożonością organizacji. Podczas gdy audyty są „zewnętrzne” dla jednostek bezpośrednio zaangażowanych w realizowaniu usługi, to nadal pozostają "wewnętrznymi" dla organizacji jako całości. Celem audytów nie jest dogłębne badanie procesów technicznych, ale raczej osiągnięcie pewności co do funkcji, czynności i zasobów zarządzania bezpieczeństwem w jednostkach liniowych. Audyty wykorzystuje się, aby zapewnić, że struktura SMS jest prawidłowa pod względem zatrudnienia, zgodności z zatwierdzonymi procedurami i instrukcjami, poziomami kompetencji i szkolenia do obsługiwania sprzętu i obiektów oraz dla utrzymania wymaganych poziomów funkcjonowania itp.

9.6.14 ***Lustracje bezpieczeństwa*** sprawdzają konkretne elementy lub procedury konkretnej operacji, takie jak obszary problemowe lub wąskie gardła w codziennych operacjach, rozumienie i opinie personelu operacyjnego oraz obszary, w których występują rozłamy lub nieporozumienia. Badania dot. bezpieczeństwa może spowodować konieczność zastosowania list kontrolnych, ankiet i nieformalnych poufnych wywiadów. Ponieważ lustracje są subiektywne, przed podjęciem działań naprawczych, konieczna może okazać się ich weryfikacja. Lustracje mogą zapewnić niedrogie źródło znaczącej informacji o bezpieczeństwie.

9.6.15 ***Wewnętrzne badania*** związane z bezpieczeństwem dotyczą zdarzeń lub incydentów, które nie muszą być badane lub zgłaszane Państwu, aczkolwiek w niektórych przypadkach organizacje mogą przeprowadzić wewnętrzne dochodzenie niezależnie od faktu, że zdarzenie, o którym mowa jest badane przez Państwo. Przykłady zdarzeń lub incydentów, które wchodzą w zakres wewnętrznych dochodzeń związanych z bezpieczeństwem to: turbulencje podczas lotu (operacje lotnicze); częste zatory (ATC); zużycie materiału (obsługa) i operacje pojazdów naziemnych na płycie lotniska.

9.6.16 Podsumowując, udział poziomu bezpieczeństwa i monitorowania źródeł informacji w SMS organizacji można zreasumować jak niżej:

a) zgłaszanie zagrożeń jest podstawowym źródłem informacji o zagrożeniach dla operacji;

b) badania dot. bezpieczeństwa są źródłem informacji o sprawach związanych z bezpieczeństwem i/lub bezpieczeństwem systemowym;

c) badania bezpieczeństwa powiązane są z zarządzaniem zmianami i zapewniają utrzymanie poziomu bezpieczeństwa w zmieniających się warunkach operacyjnych;

d) audyty zapewniają integralność struktur i procesów SMS;

e) w badaniach dot. bezpieczeństwa powołuje się opinie ekspertów i rozumienie specyficznych obszarów problemowych w codziennych operacjach;

f) wewnętrzne dochodzenia związane z bezpieczeństwem zajmują się skutkami o niewielkim znaczeniu, które nie muszą być badane przez Państwo.

### 9.7 OCHRONA ŹRÓDEŁ INFORMACJI O BEZPIECZEŃSTWIE

9.7.1 Historia bezpieczeństwa międzynarodowego lotnictwa cywilnego jest wynikiem, spośród wielu innych, dwóch podstawowych czynników: ciągłego procesu nauczania opartego na rozwoju i dobrowolnej wymianie informacji o bezpieczeństwie oraz umiejętności zamiany błędów na działania zapobiegawcze. Już dawno stwierdzono, że dążenia skierowane na ulepszenie współczesnego bezpieczeństwa lotnictwa cywilnego muszą być oparte na danych empirycznych. Jest wiele źródeł takich danych dostępnych dla lotnictwa cywilnego. W kombinacji tworzą podstawę dla rzetelnego zrozumienia silnych i słabych punktów operacji lotniczych.

9.7.2 Przez lata, informacje pozyskiwane z wypadków i incydentów tworzyły kręgosłup działań kierowanych na udoskonalanie projektu wyposażenia, procedur obsługowych, szkolenia załóg lotniczych, systemów kontroli ruchu lotniczego, funkcji i projektu lotniska, wspomagających służby pogodowe i innych, krytycznych dla bezpieczeństwa aspektów systemu transportu lotniczego. Wraz z dostępnością do środków technologicznych ostatnie lata doprowadziły do przyspieszonego rozwoju w zbieraniu danych o bezpieczeństwie, przetwarzaniu i wymianie systemów (dalej zwanych, w kombinacji z badaniami wypadków i incydentów oraz ich meldowaniu, jako systemy zbierania i przetwarzania danych o bezpieczeństwie lub SDCPS). SDCPS, jak omówiono w rozdziale 3, są niezbędne dla SMS i generują informację wykorzystywaną do wdrażania działań naprawczych w bezpieczeństwie i bieżących strategii.

9.7.3 SDCPS pozwoliły lotnictwu cywilnemu na lepsze zrozumienie błędów operacyjnych: dlaczego się zdarzają, co należy zrobić, aby ich występowanie zminimalizować i jak powstrzymać ich negatywny wpływ na bezpieczeństwo. Bezdyskusyjnym pozostaje stwierdzenie, że zagrożenia prowadzą do błędów operacyjnych w lotnictwie, z których większość jest nieodwracalna. Ludzie dobrze wyszkoleni, z dobrymi zamiarami popełniają błędy podczas obsługi, użytkowania lub kontrolowania dobrze zaprojektowanego sprzętu. Dla tych rzadkich sytuacji, w których błędy są wynikiem świadomych działań, nadużycia substancji, sabotażu lub wykroczeń, odpowiednie systemy wykonawcze zapewniają, że łańcuch odpowiedzialności nie ulega zerwaniu. To podwójne podejście, łączące poszerzone rozumienie nieodwracalnych błędów operacyjnych z odpowiednimi przepisami wykonawczymi w przypadku nadużyć, dobrze służyło lotnictwu cywilnemu w znaczeniu bezpieczeństwa, jednocześnie gwarantując, że nie ma żadnej przystani dla przestępców.

9.7.4 Ostatnie lata wykazały jednak trend, wskazujący na wykorzystywanie, przy podejmowaniu działań związanych z błędami operacyjnymi skutkującymi incydentami, informacji z SDCSP jako środka dyscyplinującego oraz egzekwującego. Dopuszczono go również jako dowód w procesach sądowych, co skutkowało oskarżeniem osób biorących udział w takich zdarzeniach. Oskarżenia kryminalne w incydentach lotniczych będących skutkiem nieodwracalnych błędów operacyjnych może utrudniać rozwój i dobrowolna wymiana informacji o bezpieczeństwie, która jest niezbędna dla usprawnienia bezpieczeństwa lotniczego.

9.7.5 Podjęto kilka inicjatyw w międzynarodowym środowisku lotnictwa cywilnego w celu podjęcia zagadnienia zabezpieczenia SDCPS. Jednak, mając na uwadze delikatność omawianej kwestii, konieczne są ramy zapewniające jedność celu i zgodność wysiłków całego lotnictwa cywilnego. Wysiłki dla ochrony informacji o bezpieczeństwie muszą wyznaczać bardzo delikatną równowagę pomiędzy potrzebą ochrony informacji o bezpieczeństwie a odpowiedzialnością wymiaru sprawiedliwości. Należy przyjąć bardzo ostrożne podejście w tym zakresie, aby uniknąć propozycji, które mogłyby być nie zgodne z prawem w zakresie zarządzania sprawiedliwością w umawiających się państwach.

9.7.6 Podczas 35 sesji Zgromadzenia ICAO rozważano temat ochrony źródeł i swobodnego przepływu informacji o bezpieczeństwie i przyjęto Rezolucję Zgromadzenia A35-17 – „Ochrona informacji z systemów zbierania i przetwarzania danych o bezpieczeństwie w celu poprawienia bezpieczeństwa lotniczego”. Rezolucja zaleciła Radzie ICAO „opracowanie odpowiednich prawnych wytycznych, które ułatwią Państwom wprowadzenie krajowych uregulowań prawnych i przepisów chroniących informacje zebrane ze wszystkich systemów zbierania i przetwarzania danych o bezpieczeństwie jednocześnie zezwalając na prawidłowe działanie wymiaru sprawiedliwości w państwie.”

9.7.7 Jako pierwszy krok w opracowywaniu prawnych wytycznych, o których mowa w Rezolucji Zgromadzenia A35-17, ICAO zwróciło się do niektórych Państw o przedstawienie przykładów ich prawa i przepisów związanych z ochroną informacji z SDCPS. Następnie ICAO przeprowadziło analizę otrzymanego od Państw materiału poszukując w dostarczonych regulacjach prawnych i przepisach wspólnych wątków i punktów pojęciowych.

9.7.8 Przygotowanie wytycznych prawnych (Dodatek E do Załącznika13 – Badanie wypadków i zdarzeń lotniczych) ma na celu wesprzeć Państwa przy wydawaniu prawa krajowego i przepisów dotyczących ochrony informacji zebranej z SDCPS, jednocześnie zezwalając na prawidłowe działanie wymiaru sprawiedliwości. Celem tego działania jest zapobieganie nieprawidłowemu wykorzystaniu informacji zebranych wyłącznie dla poprawienia bezpieczeństwa lotniczego. Mając na uwadze, że państwa mają prawo do pewnego zakresu elastyczności przy opracowywaniu swoich praw i przepisów, zgodnie z własną polityką i praktykami, pomoc prawna przyjmuje kształt serii zasad, które mogą być przyjęte dla spełnienia potrzeb Państwa przy wdrażaniu praw i przepisów dotyczących ochrony informacji o bezpieczeństwie. Poniżej krótki opis wytycznych.

9.7.9 Wytyczne prawne zawierają ogólne zasady stwierdzając, że:

a) Wyłącznym celem ochrony informacji o bezpieczeństwie przed jej nieprawidłowym wykorzystaniem jest zapewnienie jej ciągłej dostępności, tak, aby na czas podejmowano prawidłowe działania i poprawiono bezpieczeństwo lotnicze;

b) Ochrona informacji o bezpieczeństwie nie ma na celu przeszkadzać w prawidłowym działaniu wymiaru sprawiedliwości;

c) Prawo i przepisy krajowe dotyczące ochrony informacji o bezpieczeństwie powinny zapewnić utrzymanie równowagi pomiędzy potrzebą ochrony informacji o bezpieczeństwie prowadzącą do poprawienia bezpieczeństwa lotniczego, a potrzebą prawidłowego działania wymiaru sprawiedliwości;

d) Prawo i przepisy krajowe dotyczące ochrony informacji o bezpieczeństwie powinny zapobiegać jej nieprawidłowemu wykorzystaniu;

e) Zapewnienie ochrony kwalifikowanej informacji o bezpieczeństwie w oparciu o wyszczególnione warunki jest częścią obowiązków państwa w zakresie bezpieczeństwa.

9.7.10 Wytyczne zawierają zasady ochrony, jak niżej:

a) Informacja o bezpieczeństwie powinna być zakwalifikowana do jej ochrony przed nieprawidłowym wykorzystaniem zgodnie z podanymi warunkami i powinna uwzględniać, ale niekoniecznie, ograniczanie się do: informacji zbieranej wyłącznie dla celów bezpieczeństwa, której ujawnienie powstrzymałoby jej ciągłą dostępność;

b) Dla każdego SDCPS musi być szczególna ochrona oparta na charakterze zawartej w niej informacji o bezpieczeństwie;

c) Należy opracować formalną procedurę zapewniającą ochronę kwalifikowanej informacji o bezpieczeństwie, zgodnie z wyszczególnionymi warunkami;

d) Nie należy korzystać z informacji o bezpieczeństwie w inny sposób niż dla celów dla której została zebrana;

e) Wykorzystanie informacji o bezpieczeństwie w postępowaniach dyscyplinarnych, cywilnych, administracyjnych i kryminalnych może mieć miejsce tylko wówczas, gdy jest odpowiednio zabezpieczona prawem krajowym.

9.7.11 Wytyczne mówią, że odstępstwo od ochrony informacji o bezpieczeństwie może być przyznane tylko przez prawo i przepisy krajowe, gdy:

a) są dowody, że zdarzenie zostało spowodowane przez czyn, uważany przez prawo za zachowanie z zamiarem spowodowania szkód lub zachowanie ze świadomością, że jego skutkiem będą zniszczenia, równoważne z zachowaniem lekkomyślnym, zaniedbaniem lub naruszeniem z premedytacją;

b) odpowiednia władza uzna, że okoliczności możliwie wskazują, że zdarzenie mogło być spowodowane zachowaniem z zamiarem spowodowania szkód lub zachowaniem ze świadomością, że jego skutkiem będą zniszczenia, równoważne z zachowaniem lekkomyślnym, zaniedbaniem lub naruszeniem z premedytacją;

c) analiza wykonana przez odpowiednią władzę stwierdza, że przekazanie informacji o bezpieczeństwie jest konieczne dla prawidłowego działania wymiaru sprawiedliwości, i, że jej ujawnienie przeważa nad ujemnymi krajowymi i zagranicznymi skutkami takiego ujawnienia mogącymi w przyszłości mieć znaczenie dla dostępności takich informacji.

9.7.12 Wytyczne omawiają również zagadnienie przekazywania informacji do publicznej wiadomości, proponując, zgodnie z zasadami o ochronie i wyjątkami przedstawionymi powyżej, że każda osoba żądająca ujawnienia informacji o bezpieczeństwie musi swoje żądanie uzasadnić. Należy ustanowić formalne kryteria zezwalające na ujawnienie wiadomości o bezpieczeństwie, które powinny zawierać, ale nie muszą być ograniczone do poniższych:

a) ujawnienie informacji o bezpieczeństwie jest konieczne dla skorygowania/poprawienia warunków, które narażają bezpieczeństwo i/lub aby zmienić politykę i przepisy;

b) ujawnienie informacji o bezpieczeństwie nie powstrzyma przyszłej dostępności dla poprawienia bezpieczeństwa;

c) ujawnienie odnośnych informacji personalnych zawartych w informacji o bezpieczeństwie jest zgodne z odnośnymi prawami o prywatności;

d) informacja o bezpieczeństwie ujawniana jest w formie trudnej do zidentyfikowania, skróconej lub łącznej/sumarycznej.

9.7.13 Wytyczne omawiają również odpowiedzialność osoby strzegącej informacje o bezpieczeństwie, proponując, aby każdy SDCPS miał wyznaczonego „strażnika”. Osoba odpowiedzialna za informację o bezpieczeństwie jest zobowiązana do stosowania wszelkich możliwych sposobów ochrony przed jej ujawnieniem, chyba że:

a) osoba odpowiedzialna za informację o bezpieczeństwie ma zgodę autora informacji przewidzianej do ujawnienia; lub

b) osoba odpowiedzialna za informację o bezpieczeństwie jest usatysfakcjonowana tym, że ujawnienie informacji o bezpieczeństwie odbywa się zgodnie z zasadami o odstępstwie.

9.7.14 I na koniec, wytyczne omawiają ochronę informacji nagrywanych i, mając na uwadze, że wymagane prawem nagrywanie w środowisku pracy, takie jak zapis głosów w kabinie (CVR), może być odebrane przez personel operacyjny jako naruszenie prywatności, na które nie są narażani pracownicy innych zawodów, proponują aby:

a) zgodnie z zasadami ochrony i odstępstwa omówionych powyżej, prawo i przepisy krajowe powinny rozważyć wymagane prawem nagrywanie w środowisku pracy jako uprzywilejowaną, chronioną informację, tzn. informację mającą prawo do zwiększonej ochrony;

b) prawo i przepisy krajowe powinny zapewnić szczególne środki ochrony takim nagraniom z uwzględnieniem ich poufności i dostępu do nich. Środki ochrony wymaganych prawem nagrań w środowisku pracy mogą obejmować wydanie decyzji o wyłączeniu z jawności.

## 9.8 ZARZĄDZANIE ZMIANAMI

9.8.1 Organizacje lotnicze doświadczają ciągłych zmian spowodowanych rozwojem, kurczeniem się; zmianami w istniejących systemach, wyposażeniu, programach, produktach i usługach; wprowadzeniem nowego sprzętu lub procedur. Zawsze, gdy następuje zmiana można nieświadomie wprowadzić zagrożenie dla operacji. Praktyki związane z zarządzaniem bezpieczeństwem wymagają, aby zagrożenia, które stanowią produkt uboczny zmiany były systematycznie i proaktywnie identyfikowane. Należy również systematycznie opracowywać i wdrażać strategie służące zarządzaniu ryzykiem bezpieczeństwa zaistniałym w następstwie powstałych zagrożeń. Przeglądy bezpieczeństwa omówione w podrozdziale 9.6.11 stanowią cenne źródło informacji dla podejmowania decyzji w warunkach zmiany.

9.8.2 Zmiana może wprowadzić nowe zagrożenia, mieć wpływ na odpowiedniość istniejących strategii łagodzących ryzyko bezpieczeństwa i/lub na ich skuteczność. Zmiany dla organizacji mogą być zewnętrzne lub wewnętrzne. Przykłady zmian zewnętrznych to zmiany w wymaganiach prawnych, w wymaganiach ochrony i reorganizacja kontroli ruchu lotniczego. Przykłady zmian wewnętrznych to zmiany w kierownictwie, nowy sprzęt i nowe procedury.

9.8.3 Formalny proces zarządzania zmianą powinien uwzględniać poniższe trzy rozważania:

a) ***Krytyczność systemów i czynności.*** Krytyczność jest blisko związana z ryzykiem bezpieczeństwa. Krytyczność odnosi się do potencjalnych konsekwencji złego użytkowania sprzętu lub nieprawidłowo wykonanej czynności – zasadniczo odpowiadając na pytanie „jak ważny jest ten sprzęt/czynność dla bezpiecznego działania operacji?" Jest to rozważanie, które należy rozpatrzyć w trakcie procesu projektowania systemu, ale ma również znaczenie w sytuacji, gdy następuje zmiana. Jest oczywistym, że niektóre czynności są bardziej ISTOTNE dla bezpiecznej dostawy usługi niż inne. Np. zmiany w czynnościach lub procedurach związanych z przywróceniem statków powietrznych do operacji po poważnych czynnościach obsługowych wykonanych w organizacji, która dopiero co uruchomiła swoją własną organizację obsługową, a dotychczas prace obsługowe kontraktowała u podwykonawcy, można uznać za bardziej krytyczną dla bezpieczeństwa niż podobny scenariusz dotyczący zmian w działalności cateringowej. Wyposażenie i czynności, które mają wyższy stopień krytyczny dla bezpieczeństwa muszą być poddane przeglądowi po wprowadzeniu zmiany, aby zapewnić, że można podjąć działania naprawcze dla monitorowania pojawiających się potencjalnych zagrożeń.

b) ***Stabilność systemów i środowisk operacyjnych***. Zmiany mogą być skutkiem zaprogramowanych zmian takich jak rozwój, operacje do nowych portów, zmiany we flocie, zmiany w zakontraktowanych usługach lub inne zmiany będące pod bezpośrednią kontrolą organizacji. Zmiany w środowisku operacyjnym są również ważne, takie jak status ekonomiczny lub finansowy, niepokój pracowników, zmiany w środowisku politycznym lub prawnym lub w otoczeniu fizycznym, takie jak cykliczne zmiany pogodowe. Podczas gdy te czynniki nie są pod bezpośrednią kontrolą organizacji, to musi ona podjąć odpowiednie działania jako reakcję na nie. Częste zmiany w systemach lub środowisku operacyjnym dyktują konieczność częstszego uaktualniania przez kierownictwo kluczowych informacji niż ma to miejsce w sytuacjach bardziej stabilnych. Jest to istotny aspekt w zarządzaniu zmianami.

c) ***Dotychczasowe działanie***. Dotychczasowe działanie systemów krytycznych jest udowodnionym wskaźnikiem funkcjonowania w przyszłości. Jest to miejsce, w którym charakter zamkniętej pętli zapewniania bezpieczeństwa zaczyna mieć znaczenie. W procesie zapewniania bezpieczeństwa należy podjąć analizę trendów, aby prześledzić zastosowane w czasie środki dla zapewnienia bezpieczeństwa oraz przekształcenie tej informacji na przyszłe czynności do podjęcia w sytuacji gdy następuje zmiana. Ponadto, tam gdzie stwierdzono niedociągnięcia, które zostały naprawione jako skutek wykonanych audytów, ocen, badań lub meldunków, bardzo ważnym jest, aby informacja ta była rozważona dla zapewnienia skuteczności działań naprawczych.

9.8.4 Formalny proces zarządzania zmianą powinien następnie zidentyfikować zmianę w ramach organizacji, która może mieć wpływ na ustanowione procesy, procedury, wyroby i usługi. Przed wdrożeniem zmian, formalny proces zarządzania zmianą powinien opisać uzgodnienia zapewniając odpowiedni poziom bezpieczeństwa. Wynikiem tego procesu będzie obniżenie ryzyk bezpieczeństwa do poziomu ALARP, będącego skutkiem zmian w świadczeniu usług przez organizację.

9.8.5 W rozdziale 7 omówiono znaczenie opisania systemu (opis sytemu) jako jeden z fundamentalnych, wstępnych czynności w planowaniu SMS. Założeniem opisu systemu jest określenie podstawy analizy zagrożenia dla systemu podstawowego. Wraz z rozwojem systemu, pozornie małe, narastające zmiany w systemie (lub w środowisku, które dostarcza kontekst dla działania systemu) mogą na przestrzeni czasu się zakumulować, co spowoduje, że pierwotny opis systemu jest niedokładny. Tak więc jako część formalnego procesu zarządzania zmianą, opis systemu i podstawa analizy zagrożenia muszą być okresowo przeglądane, aby określić ich ciągłą ważność, nawet jeżeli nie występują okoliczności zmiany. Organizacja , gdy wprowadzane są zmiany, powinna przejrzeć swój system, jego przewidywane i aktualne środowisko operacyjne, a następnie dokonywać przeglądów okresowych, aby upewnić się, że nadal posiada jasny obraz okoliczności, w których realizowana jest dostawa usługi.

## 9.9 CIĄGŁE USPRAWNIANE SMS

9.9.1 Budowanie pewności oparte jest na zasadzie ciągłego poprawiania cyklu. Podobnie jak zapewnienie jakości umożliwia ciągłą jej poprawę, zapewnienie bezpieczeństwa zapewnia kontrolę nad jego poziomem, włącznie ze zgodnością prawną, poprzez stałą weryfikację i rozwój systemu operacyjnego. Założenia te można osiągnąć poprzez zastosowanie podobnych narzędzi: wewnętrznych ocen i niezależnych audytów (zarówno wewnętrznych jak i zewnętrznych), skrupulatnej kontroli dokumentów i ciągłego monitorowania zabezpieczeń i działań łagodzących.

9.9.2 ***Wewnętrzne oceny*** obejmują ocenę działalności operacyjnej organizacji jak również specyficznych funkcji SMS. Oceny przeprowadzane dla celu niniejszego wymagania muszą być wykonane przez osoby lub organizacje funkcjonalnie niezależne od ocenianego procesu technicznego (tzn. specjalistyczny wydział zajmujący się bezpieczeństwem lub zapewnieniem jakości lub inny wydział wskazany przez kierownictwo). Funkcja wewnętrznej oceny również wymaga przeprowadzenia audytu i oceny funkcji zarządzania bezpieczeństwem, tworzenia polityki, zarządzania ryzykiem, zapewniania bezpieczeństwa i jej promocji. Audyty te pozwalają menedżerom wskazanym jako odpowiedzialni za SMS przeprowadzić inwentaryzację procesów samego SMS.

9.9.3 ***Audyty wewnętrzne*** są ważnym narzędziem dla kierowników, wykorzystywanym do pozyskiwania informacji, w oparciu o którą mogą podejmować decyzje i utrzymywać na właściwym torze czynności operacyjne. Główna odpowiedzialność za zarządzanie bezpieczeństwem leży w gestii tych, którzy są „właścicielami" czynności technicznych organizacji wspierających realizację usług. To tutaj najczęściej pojawiają się zagrożenia, tutaj braki w czynnościach mają swój udział w ryzyku bezpieczeństwa i tutaj bezpośredni nadzór oraz przydzielanie środków może złagodzić ryzyko do poziomu ALARP. Podczas, gdy audyty wewnętrzne często są traktowane jako test lub „ocena" czynności organizacji, stanowią istotne, pomocnicze narzędzie w zapewnianiu bezpieczeństwa przez kadrę kierowniczą kierującą czynnościami wspierającymi realizacje usług kontrolującą, czy wdrożone zabezpieczenia przed ryzykiem bezpieczeństwa nadal działają i są skuteczne w ciągłym utrzymywaniu bezpieczeństwa operacyjnego.

9.9.4 ***Audyty zewnętrzne*** SMS mogą być przeprowadzone przez regulatora, partnerów code-share, organizacje klientów lub trzecią stronę wybraną przez organizację. Audyty takie zapewniają nie tylko mocny interfejs z systemem nadzoru, ale również stanowią wtórny system gwarancji.

9.9.5 W związku z tym ciągłe usprawnianie SMS ma na celu określanie bezpośrednich przyczyn działania poniżej standardów oraz ich znaczenie dla SMS oraz sytuacji naprawczych uwzględniających działanie poniżej standardów zidentyfikowane w wyniku czynności zapewnienia bezpieczeństwa. Ciągłe usprawnianie wprowadzane jest na podstawie ocen wewnętrznych, wewnętrznych i zewnętrznych audytów i ma zastosowanie do:

a) proaktywnej oceny obiektów, sprzętu, dokumentacji i procedur, np. poprzez oceny wewnętrzne;

b) proaktywnej oceny pracy/zachowania danej osoby dla zweryfikowania czy wypełnia swoje obowiązki związane z bezpieczeństwem, np. poprzez okresowe oceny kompetencji (forma oceny/audytu);

c) oceny reaktywne dla zweryfikowania skuteczności systemu pod kątem kontroli i łagodzenia ryzyka, np. przy wykorzystaniu audytu wewnętrznego i zewnętrznego.

9.9.6 W podsumowaniu, ciągłe usprawnienie może następować tylko wówczas gdy organizacja wykazuje stałą czujność w aspekcie skuteczności swoich operacji technicznych i swoich działań naprawczych. Faktycznie, bez stałego monitorowania zabezpieczeń i działań łagodzących, nie ma żadnej możliwości stwierdzenia czy proces zarządzania bezpieczeństwem spełnia swoje założenia. I podobnie, nie ma żadnej metody pomiaru, czy SMS spełnia swoje zadanie w zakresie skuteczności.

## 9.10 ZALEŻNOŚĆ POMIĘDZY ZARZĄDZANIEM RYZYKIEM BEZPIECZEŃSTWA (SRM) A ZAPEWNIANIEM BEZPIECZEŃSTWA (SA)

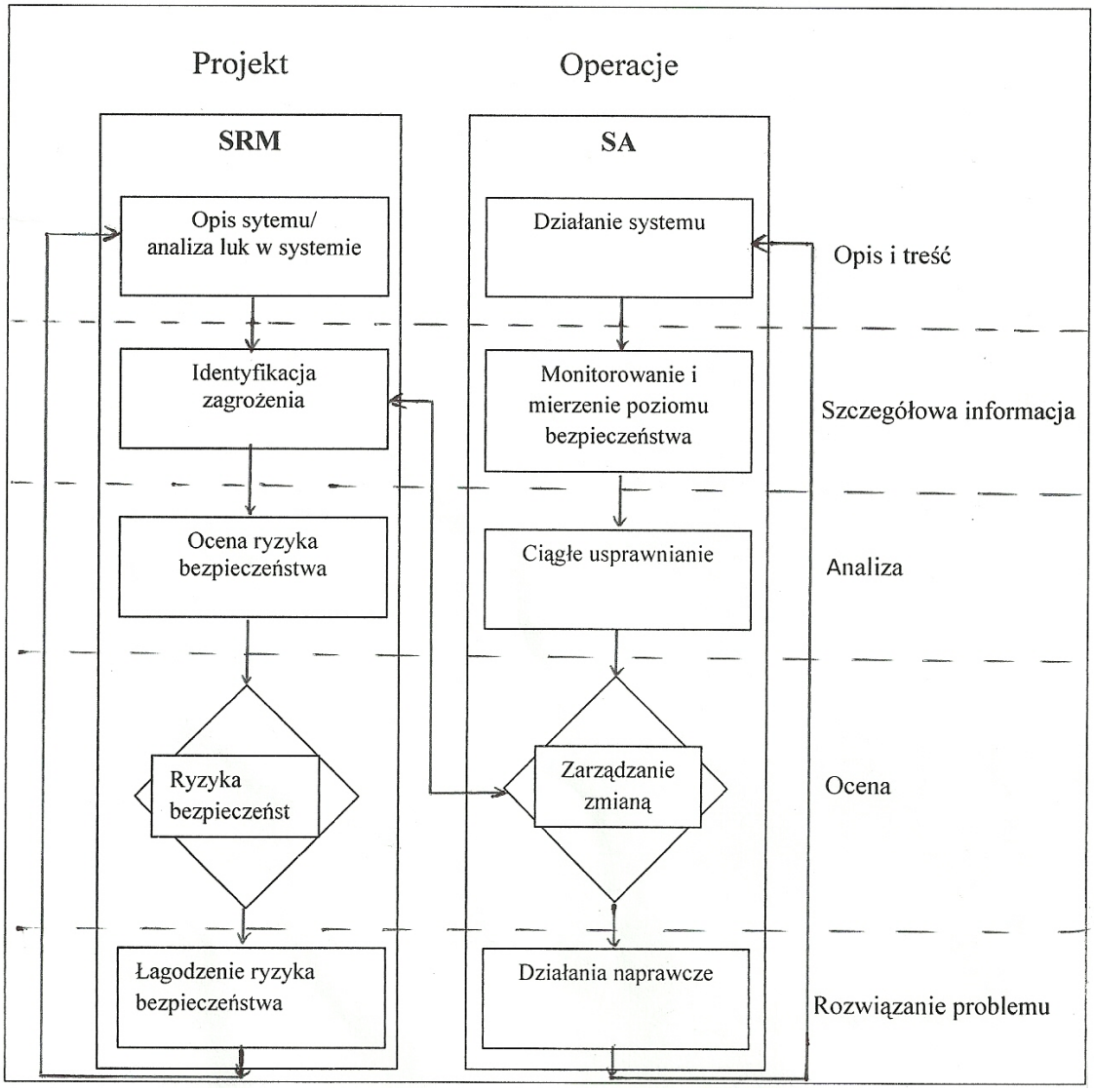
9.10.1 Subtelności we współpracy pomiędzy zarządzaniem ryzykiem a zapewnianiem bezpieczeństwa są często źródłem nieporozumień. Jednym z pierwszych zadań w skutecznym zarządzaniu ryzykiem bezpieczeństwa i zapewnieniem bezpieczeństwa dla usługodawcy i nadzorującej władzy lotniczej jest pełne/całkowite zrozumienie konfiguracji i struktury organizacyjnej systemu i jego działalności. W wyniku nieprawidłowego zaprojektowania takich działań lub słabego dopasowania systemu do jego środowiska operacyjnego powstaje poważna liczba zagrożeń i ryzyk bezpieczeństwa. W tych przypadkach występuje słabe rozumienie zagrożeń dla bezpieczeństwa operacyjnego i w związku z tym jest ono niedostatecznie kontrolowane.

9.10.2 Funkcja zarządzania ryzykiem przez SMS zapewnia wstępną identyfikację zagrożeń i ocenę ryzyka bezpieczeństwa. Opracowywane są organizacyjne zabezpieczenia przed ryzykiem bezpieczeństwa, a po stwierdzeniu, że zabezpieczenia te są w stanie sprowadzić poziom ryzyka do ALARP następuje ich wdrożenie do codziennych operacji. Teraz zadania przejmuje funkcja zapewniania bezpieczeństwa w celu potwierdzenia, że zabezpieczenia przed ryzykiem bezpieczeństwa są wykorzystywane zgodnie z założeniami i nadal spełniają założone cele. Funkcja zapewnienia bezpieczeństwa pozwala również na identyfikację zapotrzebowania na nowe zabezpieczenia przed ryzykiem bezpieczeństwa spowodowane przez zmiany w środowisku operacyjnym.

9.10.3 W SMS wymagania dla bezpieczeństwa systemu opracowywane są na podstawie obiektywnej oceny ryzyk bezpieczeństwa występujących w działalności organizacji wspierającej realizację usługi. Część systemu zajmująca się zapewnianiem skupia się na udowodnianiu przez organizację (sobie i odpowiednim stronom zewnętrznym), że wymagania te zostały spełnione, przez zbieranie i analizę obiektywnych dowodów.

9.10.4 W związku z tym, funkcja SMS w zakresie zarządzania ryzykiem umożliwia ocenę ryzyk bezpieczeństwa w operacjach wspierających świadczenie usług, jak również w opracowywaniu zabezpieczeń, aby sprowadzić ocenione ryzyko do poziomu ALARP. Funkcja ta również wspiera decyzje związane z bezpieczeństwem, a powiązane z tymi czynnościami. Po wdrożeniu, funkcja SMS w odniesieniu do zapewnienia bezpieczeństwa działa w sposób podobny do funkcji zapewniania jakości SMS. W istocie funkcje zapewnienia bezpieczeństwa SMS zostały prawie w całości wywodzą się z ISO 9001-2000, międzynarodowego standardu zarządzania jakością. Jak już wcześniej omówiono, nie ma żadnej, poważnej różnicy; podczas gdy typowe wymagania QMS są wymaganiami klienta i oparte są na jego zadowoleniu, to wymagania SMS są wymaganiami dotyczącymi bezpieczeństwa i oparte są na satysfakcji z poziomu bezpieczeństwa.

9.10.5 Należy powtórzyć role tych dwóch funkcji w ramach zintegrowanego procesu SMS. Proces zarządzania ryzykiem bezpieczeństwa (SRM) zapewnia wstępną identyfikację zagrożeń i ocenę ryzyka. Opracowywane są organizacyjne zabezpieczenia przed ryzykiem bezpieczeństwa, a po stwierdzeniu, że zabezpieczenia te są w stanie sprowadzić poziom ryzyka do ALARP następuje ich wdrożenie do codziennych operacji. Teraz zadania przejmuje funkcja zapewnienia bezpieczeństwa (SA). Zapewnienie bezpieczeństwa daje pewność, że stosowane są zabezpieczenia organizacyjne i że wszystkie zabezpieczenia nadal spełniają założone cele. Funkcja zapewnienia bezpieczeństwa pozwala również na identyfikację zapotrzebowania na nowe zabezpieczenia przed ryzykiem spowodowane zmianami w środowisku operacyjnym.




**Rysunek 9-1. Zależność pomiędzy zarządzaniem ryzykiem a zapewnianiem bezpieczeństwa**

### 9.11 PROMOWANIE BEZPIECZEŃSTWA – SZKOLENIE I EDUKACJA

9.11.1 Wysiłek organizacji włożony w zapewnienie bezpieczeństwa nie zakończy się sukcesem, jeżeli realizacja będzie obowiązkowa lub wyłącznie w drodze automatycznego/bezpośredniego wdrażania polityki. Promocja bezpieczeństwa nadaje ton i wymusza sposób zachowania człowieka i organizacji oraz wypełnia puste miejsca w polityce, procedurach i procesach organizacji uzasadniając wysiłek włożony w zapewnienie bezpieczeństwa.

9.11.2 Wiele procesów i procedur wymienionych w polityce i założeniach bezpieczeństwa oraz elementy zarządzania ryzykiem bezpieczeństwa i zapewnienia bezpieczeństwa SMS stanowią podstawę konstrukcji SMS. Jednak organizacja musi również wprowadzić procesy i procedury, które pozwolą na komunikację pomiędzy pracownikami operacyjnymi a kierownictwem. Organizacje muszą dołożyć wszelkich starań, aby wyartykułować swoje założenia/cele, przedstawić aktualny status działalności organizacji oraz znaczące wydarzenia. Ponadto organizacje muszą zapewnić środki/sposoby komunikacji pionowej w środowisku otwartości.

9.11.3 Promocja bezpieczeństwa obejmuje:

a) szkolenie i edukację, włącznie z rozwojem kompetencji w zakresie bezpieczeństwa,

b) porozumiewanie się w zakresie bezpieczeństwa.

9.11.4 Dyrektor ds. bezpieczeństwa dostarcza aktualnych informacji i zapewnia szkolenie w zagadnieniach związanych z bezpieczeństwem odnoszących się do specyficznych operacji i jednostek operacyjnych organizacji. Zapewnienie odpowiedniego szkolenia dla całego personelu, niezależnie od ich pozycji w organizacji, stanowi wskazanie o zaangażowaniu się kierownictwa w skuteczny SMS. Szkolenie z zakresu bezpieczeństwa i edukacja powinny składać się z:

a) udokumentowanego procesu identyfikującego potrzeby szkoleniowe;

b) procesu sprawdzającego skuteczność szkolenia;

c) wstępnego szkolenia (ogólne bezpieczeństwo) związanego ze specyfiką pracy;

d) uświadamianie/wstępne szkolenie obejmujące SMS, włącznie z czynnikiem ludzkim i czynnikami organizacyjnymi;

e) powtarzające się szkolenie z zakresu bezpieczeństwa.

9.11.5 Wymagania dotyczące szkolenia i działania w tym obszarze powinny być udokumentowane dla każdego obszaru działalności organizacji. Należy założyć indywidualną teczkę dotyczącą szkoleń dla każdego pracownika, włącznie z kierownictwem, która ułatwi identyfikowanie i ustalanie wymagań szkoleniowych pracownika i weryfikację już odbytego przez niego szkolenia. Programy szkoleniowe muszą być dostosowane do potrzeb i złożoności organizacji.

9.11.6 Szkolenie z zakresu bezpieczeństwa w organizacji musi zapewniać, że personel jest wyszkolony i kompetentny w wykonywaniu swoich obowiązków w zarządzaniu bezpieczeństwem. Podręcznik SMS (SMSM) musi wyszczególniać standardy wstępnego i powtarzającego się szkolenia dla personelu operacyjnego, zarządu i kierownictwa, osób zajmujących wyższe stanowiska oraz Dyrektora Odpowiedzialnego. Ilość szkoleń z zakresu bezpieczeństwa musi być odpowiednia do obowiązków danej osoby i jej zaangażowania w SMS. SMSM musi również wyszczególniać obowiązek prowadzenia szkolenia z zakresu bezpieczeństwa oraz jego treść, częstotliwość, ważność oraz zarządzanie dokumentacją o danym szkoleniu.

9.11.7 W szkoleniach z zakresu bezpieczeństwa powinno się przestrzegać zasady podejścia blokowego. Szkolenia z zakresu bezpieczeństwa dla pracowników operacyjnych powinny omawiać zagadnienia dotyczące odpowiedzialności za bezpieczeństwo, włącznie z przestrzeganiem wszystkich procedur operacyjnych i dot. bezpieczeństwa oraz rozpoznawanie, i zgłaszanie zagrożeń. Cele szkolenia powinny uwzględniać politykę bezpieczeństwa organizacji oraz podstawy SMS i ogólne omówienie. Program powinien uwzględniać definicję zagrożeń, skutków i ryzyk, procesu zarządzania ryzykiem bezpieczeństwa włącznie z rolami i odpowiedzialnością i, w zakresie podstaw, składanie meldunku bezpieczeństwa oraz system(y) raportowania o bezpieczeństwie funkcjonujące w organizacji.

9.11.8 Szkolenia z zakresu bezpieczeństwa dla dyrektorów i kierowników powinny omawiać odpowiedzialność za bezpieczeństwo włącznie z promocją SMS i angażowaniem pracowników operacyjnych w zgłaszanie zagrożeń. Poza opracowaniem założeń szkoleniowych dla personelu operacyjnego, dla dyrektorów i kierowników takie założenia powinny uwzględniać szczegółową wiedzę o procesie bezpieczeństwa, identyfikacji zagrożenia i ocenie ryzyka bezpieczeństwa oraz jego łagodzenia i zarządzania zmianami. Poza zakresem szkolenia dla pracowników operacyjnych, dyrektorzy i kierownicy powinni również zostać przeszkoleni w zakresie analizy danych bezpieczeństwa.

9.11.9 Szkolenia z zakresu bezpieczeństwa dla pracowników na wyższych stanowiskach powinny omawiać odpowiedzialność za bezpieczeństwo, włącznie ze spełnieniem krajowych i międzynarodowych wymagań bezpieczeństwa, alokacji zasobów, zapewnianiu skutecznego porozumiewania się pomiędzy departamentami w tematach związanych z bezpieczeństwem i aktywną promocję SMS. Oprócz założeń szkoleniowych dla dwóch grup pracowników już wymienionych, szkolenie dot. bezpieczeństwa dla pracowników na wyższych stanowiskach powinno omawiać zagadnienia związane z zapewnieniem bezpieczeństwa i jego promocją, dotyczące zadań i obowiązków związanych z bezpieczeństwem oraz ustanawianiem akceptowalnych poziomów bezpieczeństwa (Rys. 9-2).

9.11.10 I na koniec, szkolenia z zakresu bezpieczeństwa powinny obejmować szkolenie specjalistyczne z zakresu bezpieczeństwa dla Dyrektora Odpowiedzialnego. Takie szkolenie powinno być stosunkowo zwięzłe (nie dłuższe niż pół dnia) i powinno dostarczyć Dyrektorowi Odpowiedzialnemu ogólną wiedzę o SMS w organizacji, włącznie z rolami SMS i odpowiedzialnością, wiedzę o polityce bezpieczeństwa i jej założeniach, o zarządzaniu ryzykiem, i zapewnieniu bezpieczeństwa.

## 9.12 PROMOWANIE BEZPIECZEŃSTWA — INFORMOWANIE O BEZPIECZEŃSTWIE

9.12.1 Organizacja powinna przekazać wszystkim pracownikom operacyjnym jakie są cele SMS i jego procedury. SMS powinien być widoczny we wszystkich aspektach operacji danej organizacji wspomagających realizację usług. Dyrektor Odpowiedzialny za bezpieczeństwo powinien informować o poziomie bezpieczeństwa w biuletynach lub na odprawach. Dyrektor Odpowiedzialny za bezpieczeństwo powinien również dopilnować, aby nauka/doświadczenie wyciągnięte z badań (dochodzeń), historycznych przypadków oraz doświadczeń, zarówno wewnętrznych jak i innych organizacji była szeroko rozpowszechniana. Informacja powinna przepływać pomiędzy Dyrektorem Odpowiedzialnym za bezpieczeństwo a całym personelem operacyjnym organizacji. Utrzymanie odpowiedniego poziomu bezpieczeństwa będzie skuteczniejsze, jeżeli personel operacyjny będzie czynnie zachęcany do identyfikowania i meldowania o zagrożeniach. Tak więc, wymiana informacji dotyczącej bezpieczeństwa ma na celu:

a) dopilnowanie, aby wszyscy pracownicy byli świadomi istnienia SMS;

b) przekazywanie informacji krytycznej dla bezpieczeństwa;

c) wyjaśnienie, dlaczego podjęto konkretne działania;

d) wyjaśnienie dlaczego wprowadzono lub zmieniono procedury bezpieczeństwa;

e) przekazywanie informacji, o których „warto wiedzieć”.

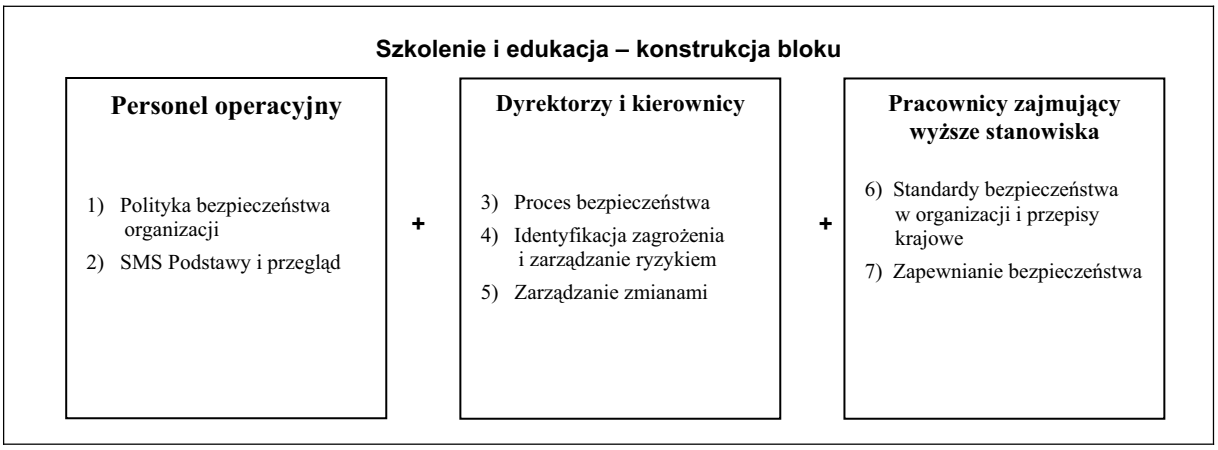
9.12.2 Przykłady wymiany informacji w organizacji obejmują:

a) podręcznik systemów zarządzania bezpieczeństwem (SMSM);

b) procesy bezpieczeństwa i procedury;

c) ulotki informacyjne o bezpieczeństwie, ogłoszenia i biuletyny;

d) stronę internetową lub e-mail.




**Rysunek 9-2. Szkolenie z zakresu bezpieczeństwa**

# Rozdział 10

# PODEJŚCIE ETAPOWE DO WDROŻENIA SMS

## 10.1 CEL I ZAWARTOŚĆ

Celem niniejszego rozdziału jest przedstawienie propozycji wdrożenia SMS w etapach. Rozdział zawiera następujące zagadnienia:

a) Dlaczego wdrażać SMS w etapach;
b) Etap I – Planowanie wdrożenia SMS;
c) Etap II – Reaktywne procesy zarządzania bezpieczeństwem;
d) Etap III – Proaktywne i przewidywalne procesy zarządzania bezpieczeństwem;
e) Etap IV – Zapewnienie bezpieczeństwa operacyjnego.

## 10.2 DLACZEGO WDRAŻAĆ SMS W ETAPACH

10.2.1 Wdrożenie SMS jest procesem bardzo prostym. Jednakże w zależności od liczby czynników, takich jak dostępność materiału pomocniczego publikowanego przez nadzorującą władzę lotniczą, wiedza o SMS wśród dostawców usług oraz środki przeznaczone na wdrożenie, bardzo prosty proces może zamienić się w przytłaczające zadanie.

10.2.2 W procesie zarządzania projektem oczywistym jest, że w przypadku projektów złożonych większe postępy uzyskuje się dzieląc złożone zadanie na mniejsze, łatwiejsze do zarządzania elementy całości. W ten sposób, przytłaczającą i często zagmatwaną złożoność oraz wynikającą z tego pracę można zamienić na prostsze i bardziej przejrzyste podzbiory zadań, z niewielkim, łatwym do zarządzania obciążeniem. I podobnie, niezbędne środki dla wdrożenia SMS „jednym rzutem", mogą być po prostu niedostępne w organizacji. Zatem, dzielenie całości na mniejsze podzbiory zadań pozwala na częściowe i mniejsze przyznanie środków dla zrealizowania podzbioru danych zadań. Częściowe przyznanie środków może być bardziej proporcjonalne do wymagań każdego zadania oraz w stosunku do środków dostępnych w organizacji. Tak więc, są dwa powody które uzasadniają propozycję wdrażania SMS w etapach:

a) zapewnienie możliwych do opanowania serii kroków, które należy wykonać podczas wdrażania SMS, włącznie z przyznawaniem środków;

b) skuteczne zarządzanie obciążeniem związanym z wdrażaniem SMS.

10.2.3 Trzeci powód, całkowicie różny od poprzednich, ale równie ważny, to unikanie „kosmetycznej zgodności". Organizacja powinna przyjąć jako swój cel, realne wdrożenie skutecznego SMS, a nie jego oznaki. Dla organizacji zbytnio obciążonej wymaganiami byłoby to bardzo atrakcyjne, by bez środków dla pełnego, całkowitego wdrożenia SMS w niewystarczającym czasie stworzyć wszystkie dokumenty, które odpowiadałyby wszystkim żądaniom i wymaganiom nadzorującej władzy lotniczej. Inaczej mówiąc, w wyniku nadmiernie wymagających przepisów, może powstać sytuacja, o której mówi się, że „zaznacza się odpowiednie kwadraciki". Jeżeli taki przypadek będzie miał miejsce, końcowy SMS, aczkolwiek kompletny i zgodny na papierze, będzie niczym innym jak pustym opakowaniem. Zapewniając serię małych, narastających i co ważne, mierzalnych kroków, zniechęca się do zgodności kosmetycznej i tylko „zaznaczania". Pełne wdrożenie SMS na pewno zajmie więcej czasu, ale odporność końcowego SMS będzie zwiększona, gdyż każdy etap wdrożenia będzie zakończony, a prostsze procesy zarządzania bezpieczeństwem będą rozpoczęte przed wdrażaniem kolejnych etapów angażujących bardziej złożone procesy zarządzania bezpieczeństwem.

10.2.4 Podsumowując, celem propozycji wdrażania SMS etapami jest:

a) zapewnienie możliwych do opanowania serii kroków, które należy wykonać podczas wdrażania SMS, włącznie z przyznawaniem środków;

b) skuteczne zarządzanie obciążeniem związanym z wdrażaniem SMS;

c) stworzenie solidnego SMS, a nie tylko prowizorycznego opakowania.

10.2.5 Proponuje się cztery etapy wdrożenia SMS. Każdy etap jest powiązany z elementem struktury SMS ICAO omówionego w rozdziale 8. Wdrożenie każdego etapu oparte jest na wprowadzeniu konkretnych składników każdego elementu struktury SMS ICAO w czasie trwania danego etapu.

### 10.3 ETAP I — PLANOWANIE WDROŻENIA SMS

10.3.1 Założeniem Etapu I procesu wdrażania SMS jest przygotowanie planu w jaki sposób zostaną spełnione wymagania i jak zostaną wprowadzone do działalności organizacji oraz planu odpowiedzialności za wdrożenie SMS.

10.3.2 Podczas Etapu I ustanawia się podstawowe planowanie i wyznacza się obowiązki. Głównym elementem Etapu I jest analiza luk w systemie. W oparciu o analizę luk w systemie, organizacja może określić aktualny stan swoich procesów zarządzania bezpieczeństwem i może przystąpić do szczegółowego planowania opracowania dalszych etapów zarządzania bezpieczeństwem. Jednym z ważniejszych efektów Etapu I jest plan wdrożenia SMS.

10.3.3 Na zakończenie Etapu I, należy zamknąć następujące czynności w taki sposób, aby spełnić oczekiwania nadzorującej władzy lotniczej, jak podano w odnośnych przepisach i materiale pomocniczym:

a) Wyznaczyć Dyrektora Odpowiedzialnego i zakres odpowiedzialności kierownictwa za bezpieczeństwo. Ta czynność oparta jest na elementach 1.1 i 1.2 struktury SMS ICAO i omówiona jest w rozdziale 8.

b) Wyznaczyć osobę (lub grupę planowania) z organizacji odpowiedzialną za wdrożenie SMS. Ta czynność oparta jest na elemencie 1.5 struktury SMS ICAO i omówiona jest w rozdziale 8.

c) Opisać system (zatwierdzone organizacje szkoleniowe, które są narażone na ryzyko bezpieczeństwa podczas świadczenia swoich usług, operatorzy statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projekt typu i/lub produkcję statku powietrznego, dostawcy usług ruchu lotniczego i certyfikowane lotniska). Ta czynność oparta jest na elemencie 1.5 struktury SMS ICAO i omówiona jest w rozdziale 7. Pomoc, jak opisać system znajduje się w Dodatku 1 do rozdziału 7.

d) Wykonać analizę luk w istniejących zasobach organizacji i porównać z krajowymi i międzynarodowymi wymaganiami dla ustanowienia SMS. Ta czynność oparta jest na elemencie 1.5 struktury SMS ICAO i omówiona jest w rozdziale 7. Wskazówki dotyczące analizy wykonywanej przez usługodawcę znajdują się w Dodatku 2 do rozdziału 7.

e) Opracować plan wdrożenia SMS, który wyjaśnia jak organizacja wdroży SMS w oparciu o przepisy krajowe i międzynarodowe SARP, opis systemu i wyniki analizy luk. Ta czynność oparta jest na elemencie 1.5 struktury SMS ICAO i omówiona jest w rozdziale 8.

f) Przygotować dokumentację zgodną z polityką bezpieczeństwa i założeniami. Ta czynność oparta jest na elemencie 1.5 struktury SMS ICAO i omówiona jest w rozdziale 8, który również zawiera przykład oświadczenia o polityce bezpieczeństwa.

g) Opracować i ustanowić sposoby wymiany informacji o bezpieczeństwie. Ta czynność oparta jest na elemencie 4.2 struktury SMS ICAO i omówiona jest w rozdziale 9.

### 10.4 ETAP II — REAKTYWNE PROCESY ZARZĄDZANIA BEZPIECZEŃSTWEM

10.4.1 Celem Etapu II jest wdrożenie zasadniczych procesów zarządzania bezpieczeństwem równocześnie poprawiając braki w istniejących procesach zarządzania bezpieczeństwem. W większości organizacji jakaś działalność w zakresie zarządzania bezpieczeństwem ma już miejsce, aczkolwiek na różnych etapach wdrożenia i o różnym stopniu skuteczności. Działania takie mogą obejmować sprawozdania z inspekcjii audytów, analizę informacji ze sprawozdań z badania incydentów oraz opracowywanie takich działań, które jeszcze nie istnieją. Ponieważ systemy przyszłościowe muszą być dopiero opracowane i wdrożone, etap ten uznawany jest jako reaktywny. Pod koniec Etapu I organizacja będzie gotowa do wykonania skoordynowanej analizy bezpieczeństwa w oparciu o informację pozyskaną przy użyciu reaktywnych metod zbierania danycho bezpieczeństwie.

10.4.2 Po zakończeniu Etapu II należy zamknąć następujące czynności w taki sposób, aby spełnić oczekiwania nadzorującej władzy lotniczej, jak podano w odnośnych przepisach i materiale pomocniczym:

a) Wdrożyć odpowiednie elementy planu SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne. Ta czynność oparta jest na elementach 2.1 i 2.2 struktury SMS ICAO i omówiona jest w rozdziałach 3, 8 i 9.

b) Opracować szkolenie odpowiednie dla elementów wdrażanego planu SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne. Ta czynność oparta jest na elementach 4.1 struktury SMS ICAO i omówiona jest w rozdziałach 3, 8 i 9.

c) Opracować dokumentację dla elementów planu wdrożenia SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne. Ta czynność oparta jest na elementach 1.5 struktury SMS ICAO i omówiona jest w rozdziałach 3, 8 i 9.

d) Opracować i ustanowić sposoby wymiany informacji o bezpieczeństwie. Ta czynność oparta jest na elemencie 4.2 struktury SMS ICAO i omówiona jest w rozdziale 9.

### 10.5 ETAP III — PROAKTYWNE I PROGNOZUJĄCE PROCESY ZARZĄDZANIA BEZPIECZEŃSTWEM

10.5.1 Celem Etapu III jest ukształtowanie prognozujących procesów zarządzania bezpieczeństwem. Zarządzanie informacją bezpieczeństwa i procesami analitycznymi jest bardzo dopracowane. Pod koniec Etapu III, organizacja będzie gotowa do wykonania skoordynowanej analizy bezpieczeństwa, w oparciu o informację pozyskaną przy użyciu reaktywnych, proaktywnych i prognozujących metod zbierania danych o bezpieczeństwie.

10.5.2 Po zakończeniu Etapu III należy zamknąć następujące czynności w taki sposób, aby spełnić oczekiwania nadzorującej władzy lotniczej, jak podano w odnośnych przepisach i materiale pomocniczym:

a) Wdrożyć te aspekty planu implementacji SMS, które odnoszą się do zarządzania ryzykiem w oparciu o procesy proaktywne i prognozujące. Ta czynność oparta jest na elementach 2.1 i 2.2 struktury SMS ICAO i omówiona jest w rozdziałach 3 i 8.

b) Opracować szkolenie odpowiednie dla elementów wdrażanego planu SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o proaktywne i prognozujące procesy. Ta czynność oparta jest na elementach 4.1 struktury SMS ICAO i omówiona jest w rozdziałach 3, 8 i 9.

c) Opracować dokumentację dla odpowiednich elementów planu wdrożenia SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne. Ta czynność oparta jest na elementach 1.5 struktury SMS ICAO i omówiona jest w rozdziałach 3, 8 i 9.

d) Opracować i ustanowić sposoby wymiany informacji o bezpieczeństwie. Ta czynność oparta jest na elemencie 4.2 struktury SMS ICAO i omówiona jest w rozdziale 9.

### 10.6 ETAP IV — ZAPEWNIENIE BEZPIECZEŃSTWA OPERACYJNEGO

10.6.1 Etap IV jest etapem zamykającym SMS. Na tym etapie ocenia się zapewnienie bezpieczeństwa operacyjnego, poprzez wdrożenie okresowego monitorowania, informacji zwrotnej i ciągłego działania korygującego w celu utrzymania skuteczności zabezpieczeń przed ryzykiem zagrożeń pojawiających się w wyniku zmieniających się wyzwań operacyjnych. Pod koniec Etapu IV zarządzanie informacją bezpieczeństwa i procesy analityczne zapewniają podtrzymywanie bezpiecznych procesów organizacyjnych w czasie i w okresach zmian w środowisku operacyjnym.

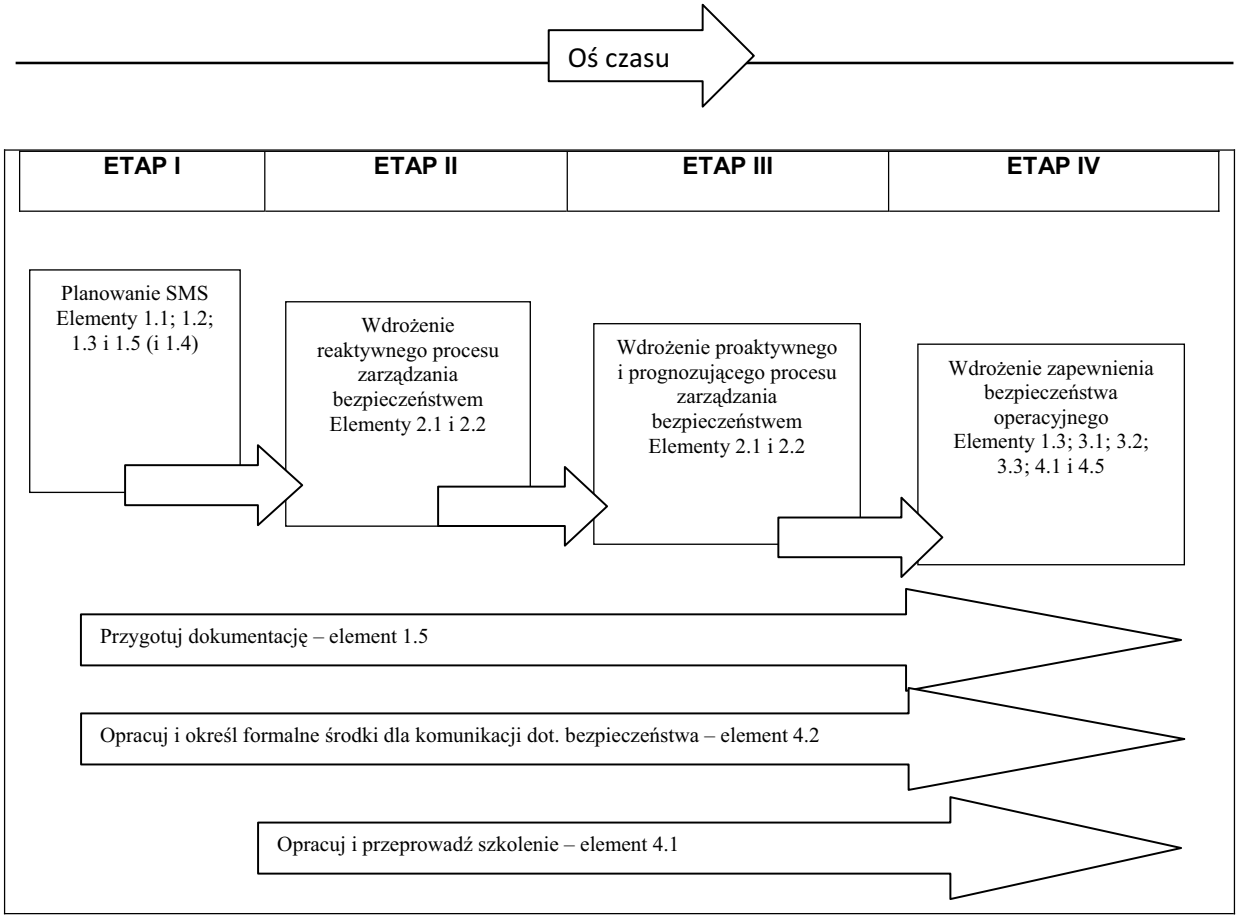
10.6.2 Po zakończeniu Etapu IV należy zamknąć następujące czynności w taki sposób, aby spełnić oczekiwania nadzorującej władzy lotniczej, jak podano w odnośnych przepisach i materiale pomocniczym:

a) Opracować i uzgodnić wskaźniki poziomu bezpieczeństwa, założenia dla poziomów bezpieczeństwa oraz system ciągłego usprawniania SMS. Ta czynność oparta jest na elementach 1.1, 3.1, 3.2 i 3.3 struktury SMS ICAO i omówiona jest w rozdziałach 6 i 9.Opracować szkolenie odpowiednie dla zapewnienia bezpieczeństwa operacyjnego. Ta czynność oparta jest na elementach 4.1 struktury SMS ICAO i omówiona jest w rozdziale 9.

c) Opracować dokumentację odpowiednią dla zapewnienia bezpieczeństwa operacyjnego. Ta czynność oparta jest na elementach 1.5 struktury SMS ICAO i omówiona jest w rozdziale 9.

d) Opracować i utrzymać formalne środki wymiany informacji o bezpieczeństwie. Ta czynność oparta jest na elemencie 4.2 struktury SMS ICAO i omówiona jest w rozdziale 9.

10.6.3 Podsumowanie kolejnych etapów wdrażania SMS i odnośnych elementów pokazana jest na rysunku 10-1.




**Rysunek 10-1. Podsumowanie kolejnych etapów wdrażania SMS**

## Dodatek 1 do Rozdziału 10

# WYTYCZNE DO OPRACOWANIA KRAJOWYCH REGULACJI DOTYCZĄCYCH SMS

### 1. PODSTAWA PRAWNA

Niniejszy przepis jest opublikowany przez ustawową władzę [odnośne przepisy dla lotnictwa cywilnego, zarządzenia dot. nawigacji lotniczej lub prawne standardy Państwa].

### 2. ZAKRES I ZASTOSOWANIE

#### 2.1 Zakres

2.1.1 Niniejszy przepis wyszczególnia wymagania dla systemu zarządzania bezpieczeństwem w organizacji usługodawcy (SMS) działającej zgodnie z Załącznikiem 1 – *Licencjonowanie Personelu*; Załącznikiem 6 – *Eksploatacja statków powietrznych*; Część I - *Międzynarodowy zarobkowy transport lotniczy – Samoloty* i Część III - *Operacje międzynarodowe – Śmigłowce*; Załącznikiem 8 - *Zdatność do lotu statków powietrznych*; Załącznikiem 11 - *Służby ruchu lotniczego*; Załącznikiem 14 – *Lotniska*, Tom I – *Budowa i eksploatacja lotnisk*.

2.1.2 W kontekście tego przepisu pojęcie “dostawca usług” odnosi się do każdej organizacji świadczącej usługi lotnicze. Pojęcie obejmuje zatwierdzone organizacje szkoleniowe narażone na operacyjne ryzyko niebezpieczeństwa w trakcie świadczenia usług, operatorów statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projekt typu i/lub produkcję statku powietrznego, dostawców służb ruchu lotniczego i certyfikowane lotniska, co będzie miało zastosowanie.

2.1.3 Niniejszy przepis zajmuje się procesami, procedurami i działaniami związanymi z bezpieczeństwem lotniczym, a nie bezpieczeństwem pracy, ochroną środowiska, obsługą klienta lub jakością produktu.

2.1.4 Dostawca usług odpowiedzialny jest za bezpieczeństwo zakontraktowanych lub zleconych podwykonawcy usług lub produktów lub tych zakupionych w innych organizacjach.

2.1.5 Niniejszy przepis określa minimalne, akceptowalne wymagania; dostawca usług może ustanowić bardziej rygorystyczne wymagania.

#### 2.2 Zakres obowiązywania i akceptacja

2.2.1 W dniu wejścia w życie [data(y)], dostawca usług będzie miał ustanowiony system zarządzania bezpieczeństwem (SMS) akceptowalny przez [Państwo], który jako minimum:

2.2.1.1 identyfikuje zagrożenia bezpieczeństwa;

2.2.1.2 zapewnia wdrożenie działań naprawczych koniecznych do utrzymania uzgodnionego poziomu bezpieczeństwa;

2.2.1.3 zapewnia ciągłe monitorowanie i regularną ocenę poziomu bezpieczeństwa;

2.2.1.4 dąży do stałego usprawniania całościowego funkcjonowania systemu zarządzania bezpieczeństwem.

2.2.2 Aby Państwo zaakceptowało SMS usługodawcy, SMS musi spełnić wymagania ustanowione niniejszym przepisem.

*Uwaga. – Przepis dotyczący SMS powinien zawierać informację dotyczącą procesu akceptacji SMS. Proces przyjęcia powinien zawierać, jak to będzie miało zastosowanie, wniosek o akceptację SMS, procedury składania wniosku o przyjęcie, czas ważności akceptacji, procedury dla wznowienia, zawieszenia lub cofnięcia akceptacji.*

## 3. ODNIESIENIA

3.1 Niniejszy przepis jest zgodny z Załącznikiem 1 – *Licencjonowanie Personelu*; Załącznikiem 6 – *Eksploatacja statków powietrznych*; Część I - *Międzynarodowy zarobkowy transport lotniczy – Samoloty* i Część III - *Operacje międzynarodowe – Śmigłowce*; Załącznikiem 8 - *Zdatność do lotu statków powietrznych*; Załącznikiem 11 - *Służby ruchu lotniczego*; i Załącznikiem 14 – *Lotniska*, Tom I – *Budowa i eksploatacja lotnisk* oraz *Podręcznikiem Zarządzania Bezpieczeństwem ICAO (Doc 9859).*

3.2 Niniejszy przepis jest zgodny z *[odnośnym prawem i/lub materiałem pomocniczym Państwa].*

## 4. DEFINICJE

*Uwaga.— Niniejszy wykaz stanowi tylko wskazówkę.*

- Wypadek
- Akceptowalny poziom bezpieczeństwa (ALoS)
- Dyrektor Odpowiedzialny
- Skutek/konsekwencja
- Stałe monitorowanie
- Analiza luk
- Zagrożenia
- Incydent
- Wewnętrzne badanie bezpieczeństwa
- Łagodzenie
- Zdarzenie
- Nadzór
- Prognozujący
- Pro aktywny
- Prawdopodobieństwo
- Procedura
- Proces
- Reaktywny
- Ryzyko
- Ocena bezpieczeństwa
- Zapewnienie bezpieczeństwa

- Audyt bezpieczeństwa
- Dyrektor ds. bezpieczeństwa
- Poziom bezpieczeństwa
- Wskaźnik poziomu bezpieczeństwa
- Założenia dla poziomu funkcjonowania
- Polityka bezpieczeństwa
- Wymaganie bezpieczeństwa
- Ryzyko bezpieczeństwa
- Lustracja bezpieczeństwa
- System Zarządzania Bezpieczeństwem (SMS)
- Krajowy Program Bezpieczeństwa (SSP)
- Dotkliwość
- Opis systemu.

## 5. UWAGI OGÓLNE

Dostawca usług opracuje, ustanowi, utrzyma i będzie przestrzegać systemu zarządzania bezpieczeństwem (SMS), który jest odpowiedni dla wielkości, charakteru i złożoności operacji, które ma prawo realizować w oparciu o swój certyfikat operacyjny oraz w oparciu o zagrożenia i ryzyko bezpieczeństwa związane z operacjami.

## 6. POLITYKA BEZPIECZEŃSTWA I JEJ ZAŁOŻENIA

### 6.1 Wymagania ogólne

6.1.1 Dostawca usług określi politykę bezpieczeństwa organizacji.

6.1.2 Polityka bezpieczeństwa będzie podpisana przez Dyrektora Odpowiedzialnego w organizacji.

6.1.3 Polityka bezpieczeństwa będzie zawierać opis odpowiedzialności zarządu i pracowników w zakresie poziomu bezpieczeństwa SMS.

6.1.4 Polityka bezpieczeństwa będzie zawierać czytelne oświadczenie o zapewnieniu odpowiednich środków dla jej wdrożenia.

6.1.5 Polityka bezpieczeństwa zostanie ogłoszona z wyraźnym poparciem całej organizacji.

6.1.6 Polityka bezpieczeństwa będzie zawierać między innymi:

6.1.6.1 zobowiązanie do ciągłego polepszania poziomu bezpieczeństwa;

6.1.6.2 procedurę zgłaszania zagrożeń;

6.1.6.3 warunki, w których działania dyscyplinarne nie będą miały zastosowania w następstwie zgłoszenia zagrożenia przez pracowników.

6.1.7 Polityka bezpieczeństwa będzie zgodna, ze wszystkimi mającymi zastosowanie i obowiązującymi wymaganiami i międzynarodowymi standardami, najlepszymi praktykami przemysłu i będzie odzwierciedlać zobowiązania organizacji w zakresie bezpieczeństwa.

6.1.8 Polityka bezpieczeństwa będzie okresowo przeglądana, aby zapewnić, że pozostaje zgodna i odpowiednia dla organizacji.

6.1.9 Dostawca usług określi założenia bezpieczeństwa dla SMS.

6.1.10 Założenia bezpieczeństwa powinny być powiązane ze wskaźnikami poziomu bezpieczeństwa, poziomu funkcjonowania i planami działania SMS usługodawcy.

**6.2 Uzgodnienia organizacyjne dotyczące SMS oraz odpowiedzialność za bezpieczeństwo i obowiązki.**

6.2.1 Dostawca usług wskaże Dyrektora Odpowiedzialnego, który w jego imieniu będzie odpowiedzialny i będzie miał obowiązek spełnienia niniejszego przepisu, i przekaże [Państwu] jego nazwisko.

6.2.2 Dyrektor Odpowiedzialny będzie pojedynczą, rozpoznawalną osobą, która niezależnie od innych pełnionych funkcji, będzie miała obowiązek i będzie odpowiedzialna za wdrożenie i utrzymanie SMS w imieniu [organizacji].

6.2.3 Dyrektor Odpowiedzialny będzie miał:

6.2.3.1 pełną kontrolę nad środkami potrzebnymi dla wykonywania operacji dopuszczonych certyfikatem operacyjnym;

6.2.3.2 pełną kontrolę nad środkami finansowymi potrzebnymi dla wykonywania operacji dopuszczonych certyfikatem operacyjnym;

6.2.3.3 ostateczną władzę nad wykonywanymi operacjami dopuszczonymi certyfikatem operacyjnym;

6.2.3.4 bezpośrednią odpowiedzialność za realizację bieżących spraw organizacji;

6.2.3.5 ostateczną odpowiedzialność za zagadnienia związane z bezpieczeństwem.

6.2.4 Dostawca usług ustanowi odpowiednie porozumienia organizacyjne dla wdrożenia, przestrzegania i utrzymania funkcjonowania SMS w organizacji.

6.2.5 Dostawca usług określi odpowiedzialność, obowiązki i zakres zarządzania zarówno dla wszystkich członków zarządu, jak i pracowników, niezależnie od ich obowiązków.

6.2.6 Odpowiedzialność, obowiązki i zakres zarządzania będą zdefiniowane, udokumentowane i odnośna informacji przekazana będzie do organizacji.

6.2.7 Dostawca usług wskaże osobę z kierownictwa jako Dyrektora ds. bezpieczeństwa, osobę będącą punktem kontaktowym, odpowiedzialnym za wdrożenie i obsługę skutecznego SMS.

6.2.8 Dyrektor ds. bezpieczeństwa będzie między innymi:

6.2.8.1 pilnował, aby potrzebne dla SMS procesy były opracowane, wdrożone, przestrzegane i utrzymywane;

6.2.8.2 meldował Dyrektorowi Odpowiedzialnemu o działaniu SMS i wszelkiej konieczności jego usprawnienia;

6.2.8.3 promował bezpieczeństwo w całej organizacji.

### 6.3 Koordynacja planowania reagowania w sytuacjach awaryjnych

6.3.1 Dostawca usług dopilnuje, aby jego plan reagowania w sytuacjach awaryjnych był odpowiednio skoordynowany z planami reagowania w sytuacjach awaryjnych tych organizacji, z którymi musi współpracować podczas realizacji swoich usług.

6.3.2 Koordynacja planu reagowania w sytuacjach awaryjnych zapewni uporządkowane i skuteczne przejście z operacji normalnych do awaryjnych, a następnie powrót do normalnych.

6.3.3 Koordynacja planu reagowania w sytuacjach awaryjnych będzie między innymi zawierać:

6.3.3.1 przekazanie władzy w sytuacji awaryjnej;

6.3.3.2 przypisanie podczas skoordynowanych działań obowiązków stosownych do sytuacji awaryjnej;

6.3.3.3 koordynację wysiłków, aby podołać sytuacji awaryjnej;

6.3.3.4 kompatybilność z planami reagowania w sytuacjach awaryjnych innych organizacji.

### 6.4 Dokumentacja

6.4.1 Dostawca usług opracuje i będzie utrzymywać dokumentację SMS, tak, aby zawierała:

6.4.1.1 politykę bezpieczeństwa i założenia;

6.4.1.2 wymagania SMS;

6.4.1.3 procesy i procedury SMS;

6.4.1.4 obowiązki oraz informację o tym, kto zarządza procesami i procedurami;

6.4.1.5 efekty SMS.

6.4.2 Dostawca usług, jako część dokumentacji SMS, opracuje pełny opis systemu.

6.4.3 Opis system będzie zawierać następujące informacje:

6.4.3.1 interakcje systemu z innymi systemami w systemie transportu lotniczego;

6.4.3.2 funkcję systemu;

6.4.3.3 wymagania systemu operacyjnego odnośnie rozważanych możliwości człowieka;

6.4.3.4 oprzyrządowanie systemu;

6.4.3.5 oprogramowanie systemu;

6.4.3.6 powiązane procedury dla funkcjonowania i korzystania z systemu;

6.4.3.7 środowisko operacyjne;

6.4.3.8 zakontraktowane, zamówione u podwykonawcy i kupione wyroby i/lub usługi.

6.4.4 Dostawca usług, jako część dokumentacji SMS, wykona analizę luk w systemie w celu:

6.4.4.1 zidentyfikowania uzgodnień dotyczących bezpieczeństwa i struktur już istniejących w organizacji;

6.4.4.2 określi dodatkowe uzgodnienia dotyczące bezpieczeństwa, konieczne do wdrożenia i utrzymania funkcjonowania SMS w organizacji.

6.4.5 Dostawca usług, jako część dokumentacji SMS, opracuje, będzie przestrzegać i utrzymywać plan wdrożenia SMS.

6.4.6 Plan wdrożenia SMS będzie definicją podejścia jaką organizacja przyjmie dla zarządzania bezpieczeństwem w sposób spełniający założenia bezpieczeństwa organizacji.

6.4.7 Plan wdrożenia SMS w sposób jednoznaczny omówi współpracę pomiędzy SMS usługodawcy a systemami innych organizacji, z którymi dostawca usług musi współpracować w trakcie realizacji usług.

6.4.8 Plan wdrożenia SMS zawierać będzie następujące elementy:

6.4.8.1 politykę bezpieczeństwa i cele;

6.4.8.2 opis systemu;

6.4.8.3 analizę luk w systemie;

6.4.8.4 elementy SMS;

6.4.8.5 zadania bezpieczeństwa i odpowiedzialności;

6.4.8.6 politykę meldowania o zagrożeniach;

6.4.8.7 sposób zaangażowania pracowników;

6.4.8.8 sposób mierzenia poziomu bezpieczeństwa;

6.4.8.9 szkolenie z zakresu bezpieczeństwa;

6.4.8.10 wymianę informacji o bezpieczeństwie;

6.4.8.11 przegląd poziomu bezpieczeństwa przez zarząd.

6.4.9 Plan wdrożenia SMS będzie zatwierdzony przez osoby zajmujące wyższe stanowiska w organizacji.

6.4.10 Dostawca usług, jako część dokumentacji SMS, opracuje i będzie utrzymywać podręcznik zarządzania systemami bezpieczeństwa (SMSM), w celu poinformowania całej organizacji o jej podejściu do bezpieczeństwa.

6.4.11 SMSM będzie dokumentował wszystkie aspekty SMS i będzie zawierać następujące elementy:

6.4.11.1 zakres systemu zarządzania bezpieczeństwem;

6.4.11.2 politykę bezpieczeństwa i cele;

6.4.11.3 odpowiedzialności za bezpieczeństwo;

6.4.11.4 kluczowy personel związany z bezpieczeństwem;

6.4.11.5 procedury kontroli dokumentacji;

6.4.11.6 koordynację planowania reagowania w sytuacjach awaryjnych;

6.4.11.7 programy identyfikacji zagrożenia i zarządzania ryzykiem bezpieczeństwa;

6.4.11.8 monitorowanie poziomu bezpieczeństwa;

6.4.11.9 audytowanie bezpieczeństwa;

6.4.11.10 procedury zarządzania zmianami;

6.4.11.11 promocja bezpieczeństwa;

6.4.11.12 kontrola zakontraktowanych czynności.

*Uwaga.— Ogólne wytyczne dla opracowania i utrzymywania dokumentacji SMS można znaleźć w Załącznik H do Aneksu 6, Część I ICAO, i Załącznik G (System dokumentów dotyczących bezpieczeństwa lotów) do Aneksu 6, Część III ICAO, System Dokumentacji Bezpieczeństwa Lotniczego Operatora (Operator's Flight Safety Documents System).*

## 7. ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA

### 7.1 Uwagi ogólne

7.1.1 Dostawca usług przygotuje i będzie utrzymywać formalną procedurę zapewniającą, że zagrożenia w operacjach są zidentyfikowane.

7.1.2 Dostawca usług przygotuje i będzie utrzymywać system zbierania danych o bezpieczeństwie i ich przetwarzania (*Safety Data Collection and Processing System* (SDCPS)), zezwalający na identyfikację zagrożeń oraz analizę, ocenę i łagodzenie ryzyka bezpieczeństwa.

7.1.3 SDCPS usługodawcy będzie zawierać reaktywne, proaktywne i prognozujące metody zbierania danych o bezpieczeństwie.

### 7.2 Identyfikacja zagrożenia

7.2.1 Dostawca usług przygotuje i będzie utrzymywać prawne sposoby dla skutecznego zbierania, rejestrowania, reagowania i generowania informacji zwrotnej o zagrożeniach w operacjach, które będą w sobie łączyć reaktywne, proaktywne i prognozujące metody zbierania danych o bezpieczeństwie. Prawne sposoby zbierania danych obejmować będą obowiązkowe, dobrowolne i poufne systemy zgłaszania.

7.2.2 Proces identyfikacji zagrożenia będzie składał się z następujących kroków:

7.2.2.1 zgłaszania zagrożeń, wydarzeń i obaw związanych z bezpieczeństwem;

7.2.2.2 zbieranie i przechowywanie danych o bezpieczeństwie;

7.2.2.3 analizę danych bezpieczeństwa;

7.2.2.4 upowszechnianie informacji o bezpieczeństwie wydobytych z bazy danych.

### 7.3 Ocena ryzyka bezpieczeństwa i łagodzenie

7.3.1 Dostawca usług przygotuje i będzie utrzymywał formalny proces umożliwiający wykonanie analizy, oceny i kontroli ryzyka bezpieczeństwa będącego konsekwencją zagrożeń powstających w trakcie świadczenia usług.

7.3.2 Ryzyko bezpieczeństwa będącego konsekwencją każdego zagrożenia zidentyfikowanego w procesie identyfikacji zagrożenia, opisanego w sekcji 7.2 niniejszego przepisu, będzie poddane analizie pod kątem prawdopodobieństwa jego wystąpienia i jego surowości oraz tolerancji.

7.3.3 Organizacja zdefiniuje poziomy zarządzania mające prawo podejmowania decyzji o tolerancji ryzyka bezpieczeństwa.

7.3.4 Organizacja zdefiniuje zabezpieczenia dla każdego ryzyka niebezpieczeństwa ocenianego jako dopuszczalne.

## 8. ZAPEWNIENIE BEZPIECZEŃSTWA

### 8.1 Uwagi Ogólne

8.1.1 Dostawca usług przygotuje i będzie utrzymywał procesy zapewnienia bezpieczeństwa, tak, aby zapewnić, że zabezpieczenia ryzyka bezpieczeństwa wdrożone jako efekt identyfikacji zagrożeń oraz czynności zarządzania ryzykiem bezpieczeństwa z paragrafu 7 spełniają zamierzone założenia.

8.1.2 Procedury zapewniania bezpieczeństwa będą miały zastosowanie do SMS niezależnie od tego, czy czynności i/lub operacje realizowane są wewnętrznie czy zlecone dostawcy zewnętrznemu.

### 8.2 Monitorowanie i mierzenie poziomu bezpieczeństwa

8.2.1 Dostawca usług, jako część działalności SMS związanego z zapewnianiem bezpieczeństwa, wyznaczy i będzie utrzymywać niezbędne narzędzia do weryfikacji poziomu bezpieczeństwa w odniesieniu do wskaźników i założeń poziomu bezpieczeństwa SMS i akceptowania skuteczności zabezpieczeń przed ryzykiem bezpieczeństwa.

8.2.2 Narzędzia do monitorowania i mierzenia poziomu bezpieczeństwa będą uwzględniać następujące elementy:

8.2.2.1 systemy zgłaszania zagrożenia;

8.2.2.2 audyty bezpieczeństwa;

8.2.2.3 badania bezpieczeństwa;

8.2.2.4 lustracje bezpieczeństwa;

8.2.2.5 analizy badawcze bezpieczeństwa;

8.2.2.6 wewnętrzne dochodzenia w sprawach bezpieczeństwa.

8.2.3 Procedury zgłaszania zagrożenia określą warunki zapewniające skuteczne zgłaszanie włącznie z warunkami, w których nie mają zastosowania działania dyscyplinarne/administracyjne.

### 8.3 Zarządzanie zmianami

8.3.1 Dostawca usług, jako część działalności SMS związanego z zapewnianiem bezpieczeństwa, określi i będzie utrzymywać legalny proces zarządzania zmianą.

8.3.2 Formalny proces zarządzania zmianą będzie:

8.3.2.1 identyfikował zmiany w organizacji, które mogą mieć wpływ na ustanowione procesy i usługi;

8.3.2.2 określał działania zapewniające odpowiedni poziom bezpieczeństwa przed wdrożeniem zmiany;

8.3.2.3 eliminował lub modyfikował zabezpieczenie ryzyka bezpieczeństwa, które nie są już potrzebne w związku ze zmianami w środowisku operacyjnym.

### 8.4 Ciągłe usprawnianie systemu bezpieczeństwa

8.4.1 Dostawca usług, jako część działalności SMS związanego z zapewnianiem bezpieczeństwa, opracuje i będzie utrzymywał legalny proces identyfikacji przyczyn funkcjonowania SMS poniżej standardu, określi ich implikacje na działanie SMS oraz naprawi/skoryguje/usprawni sytuacje, w których występuje działanie poniżej standardu, dla zapewnienia ciągłego usprawniania SMS.

8.4.2 Ciągłe usprawnianie SMS usługodawcy będzie obejmować:

8.4.2.1 proaktywne i reaktywne oceny obiektów, sprzętu, dokumentacji i procedur dla zweryfikowania skuteczności strategii kontroli ryzyka bezpieczeństwa;

8.4.2.2 proaktywną ocenę działania danej osoby celem weryfikacji wypełniania obowiązków dotyczących bezpieczeństwa.

## 9. PROMOWANIE BEZPIECZEŃSTWA

### 9.1 Uwagi ogólne

Wszyscy świadczący ogólne usługi opracują i będą utrzymywać formalną działalność związaną ze szkoleniem i wymianą informacji w zakresie bezpieczeństwa w celu stworzenia środowiska, w którym można spełnić założenia bezpieczeństwa określone przez daną organizację.

### 9.2 Szkolenie w zakresie bezpieczeństwa

9.2.1 Dostawca usług, jako część swojej działalności w promowaniu bezpieczeństwa, opracuje i będzie utrzymywał program szkolenia, który zapewni, że pracownicy będą wyszkoleni i kompetentni do wykonywania swoich obowiązków wynikających z SMS.

9.2.2 Zakres szkolenia odnośnie bezpieczeństwa będzie odpowiedni dla osoby zaangażowanej w SMS.

9.2.3 Świadomość bezpieczeństwa stanowić będzie podstawę dla Dyrektora Odpowiedzialnego w odniesieniu do:

9.2.3.1 założeń i polityki bezpieczeństwa;

9.2.3.2 zadań i obowiązków SMS;

9.2.3.3 standardów SMS;

9.2.3.4 zapewnienia bezpieczeństwa.

### 9.3 Wymiana informacji o bezpieczeństwie

9.3.1 Dostawca usług, jako część swojej działalność w promowaniu bezpieczeństwa opracuje i będzie utrzymywał oficjalne ścieżki wymiany informacji o bezpieczeństwie tak, aby:

9.3.1.1 zapewnić, że cały personel będzie w pełni świadomy istnienia SMS;

9.3.1.2 przekazywać krytyczną informację związaną z bezpieczeństwem;

9.3.1.3 wytłumaczyć przyczyny podjęcia konkretnych działań w zakresie bezpieczeństwa;

9.3.1.4 wytłumaczyć dlaczego wprowadzane są lub zmieniane procedury bezpieczeństwa;

9.3.1.5 przekazywać rodzajowe informacje dot. bezpieczeństwa.

9.3.2 Oficjalne ścieżki wymiany informacji będą, między innymi, uwzględniać:

9.3.2.1 politykę bezpieczeństwa i procedury;

9.3.2.2 ulotki;

9.3.2.3 biuletyny;

9.3.2.4 strony internetowe.

## 10. POLITYKA JAKOŚCI

Dostawca usług zapewni, że polityka jakości organizacji jest zbieżna z SMS oraz wspiera realizację jego zadań.

.

## 11. WDROŻENIE SMS

11.1 Niniejszy przepis proponuje, ale nie nakazuje usługodawcy zobowiązanym do wdrożenie SMS w czterech etapach, jak omówiono w 11.2 do 11.5.

11.2 ***Etap I*** — Wynikiem planowania powinien być opracowany plan omawiający sposób spełnienia wymagań, ich wdrożenie do działalności organizacji oraz schemat odpowiedzialności za wdrożenie SMS:

11.2.1 Wyznaczenie Dyrektora Odpowiedzialnego i zakresu jego odpowiedzialności za bezpieczeństwo;

11.2.2 Wyznaczenie w danej organizacji osoby (lub grupy planowania) odpowiedzialnej za wdrożenie SMS;

11.2.3 Opisanie systemu (zatwierdzone organizacje szkoleniowe, które są narażone na ryzyko bezpieczeństwa podczas świadczenia swoich usług, operatorzy statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projekt typu i/lub produkcję statku powietrznego, dostawcy usług ruchu lotniczego i certyfikowane lotniska);

11.2.4 Przeprowadzenie analizy luk w istniejących zasobach organizacji i porównanie ich z krajowymi i międzynarodowymi wymogami dla wdrożenia SMS;

11.2.5 Opracowanie planu implementacji SMS, który wyjaśni w jaki sposób organizacja wdroży SMS w oparciu o przepisy krajowe i międzynarodowe SARP, opis systemu i wyniki analizy luk w systemie;

11.2.6 Przygotowanie dokumentacji zgodnej z polityką bezpieczeństwa i jej założeniami;

11.2.7 Opracowanie i ustanowienie sposobów wymiany informacji dot. bezpieczeństwa.

11.3 ***Etap II*** — Procesy reaktywne powinny wprowadzić w życie te elementy planu wdrażania SMS, które odnoszą się do zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne:

11.3.1 identyfikacja zagrożenia i zarządzanie ryzykiem bezpieczeństwa przy wykorzystaniu procesów reaktywnych;

11.3.2 szkolenie obejmujące:

11.3.2.1 elementy planu wdrażania SMS;

11.3.2.2 zarządzanie ryzykiem bezpieczeństwa (procesy reaktywne).

11.3.3 dokumentację obejmującą:

11.3.3.1 elementy planu wdrażania SMS;

11.3.3.2 zarządzanie ryzykiem bezpieczeństwa (procesy reaktywne).

11.4 ***Etap III*** — Procesy proaktywne i prognozujące, powinny wprowadzić w życie te elementy planu wdrażania SMS, które odnoszą się do zarządzania ryzykiem bezpieczeństwa, w oparciu o procesy proaktywne i prognozujące:

11.4.1 identyfikacja zagrożenia i zarządzanie ryzykiem bezpieczeństwa przy wykorzystaniu procesów proaktywnych i prognozujących;

11.4.2 szkolenie obejmujące:

11.4.2.1 elementy planu wdrażania SMS;

11.4.2.2 zarządzania ryzykiem bezpieczeństwa (procesy reaktywne).

11.4.3 dokumentację obejmującą:

11.4.3.1 elementy planu wdrażania SMS;

11.4.3.2 zarządzania ryzykiem bezpieczeństwa (procesy reaktywne).

11.5 elementy: ***Etap IV*** — Operacyjne zapewnienie bezpieczeństwa powinno w praktyce zapewnić następujące

11.5.1 opracowanie i uzgodnienie wskaźników i celów poziomu bezpieczeństwa;

11.5.2 proces ciągłego usprawniania SMS;

11.5.3 odpowiednie szkolenie zapewniające bezpieczeństwo operacyjne;

11.5.4 dokumentację związaną z zapewnieniem bezpieczeństwa operacyjnego;

11.5.5 określenie i utrzymanie formalnych środków w celu wymiany informacji o bezpieczeństwie.

– – – – – – – – – –

## Dodatek 2 do Rozdziału 10

# WYTYCZNE DO OPRACOWANIA PLANU WDRAŻANIA SMS DLA DOSTAWCÓW USŁUG

### KONTEKST

1. Niniejszy Dodatek zawiera wytyczne ułatwiające usługodawcom opracowanie planu wdrożenia SMS, który określa podejście organizacji do zarządzania bezpieczeństwem. Plan wdrożenia SMS będzie parafowany prze personel kierowniczy organizacji i opracowany w oparciu o przepisy krajowe, międzynarodowe normy i zalecane metody postępowania (SARP), opis systemu i wyników analizy luk w systemie.

2. Opracowanie planu wdrożenia SMS:

a) wesprze dostawcę usług w opracowaniu realistycznej strategii do wdrożenia SMS, który spełni założenia bezpieczeństwa organizacji;

b) zapewni serię możliwych do zarządzania kroków wdrażania SMS;

c) stworzy schemat odpowiedzialności za wdrożenie SMS.

3. Proponuje się podejście etapowe do obowiązków związanych z wdrażaniem SMS, w celu wsparcia skutecznego zarządzania systemem. Każdy etap oparty jest na wprowadzeniu poszczególnych elementów ICAO'wskiej struktury SMS.

4. Czas wdrożenia każdego etapu będzie odpowiedni dla wielkości organizacji i złożoności oferowanych usług.

*Uwaga 1. – Wykres modelu Gannta dla opracowania planu wdrożenia SMS stanowi załącznik do niniejszego Dodatku. Niniejsze wytyczne stanowią tylko odniesienie, a SMS może być dopasowany do potrzeb pojedynczych usługodawców. Akta zarządzania projektem modelu Gannta są dostępne na stronie internetowej www.icao.int/fsix lub www.icao.int/anb/safetymanagement*.

*Uwaga 2. – W odniesieniu do kontekstu niniejszego Dodatku pojęcie „dostawca usług" odnosi się do każdej organizacji świadczącej usługi lotnicze. Pojęcie obejmuje: zatwierdzone organizacje szkoleniowe, które są narażone na ryzyko bezpieczeństwa podczas świadczenia swoich usług, operatorów statków powietrznych, zatwierdzonych organizacji obsługowych, organizacji odpowiedzialnych za projekt typu i/lub produkcję statku powietrznego, dostawców usług ruchu lotniczego oraz certyfikowanych lotnisk.*

## Plan wdrożenia SMS

### 1. Etap I — PLANOWANIE WDROŻENIA SMS

1.1 ***Dyrektor Odpowiedzialny***

- Wyznaczyć Dyrektora Odpowiedzialnego i osobę lub grupę planowania do opracowania planu wdrożenia SMS (jak omówiono w Rozdziale 8).

1.2 ***Opis i analiza luk w systemie*** (jak omówiono w Rozdziale 7).

*Opis systemu*

- Wykonaj opis systemu, co stanowi pierwszą, wstępną czynność dla przygotowania SMS w organizacji. Opis powinien zawierać zasady współpracy w ramach systemu jak i z innymi systemami transportu lotniczego. Wytyczne dla przygotowania opisu systemu znajdują się w Dodatku 1 do Rozdziału 7.

*Analiza luk w systemie*

- Wykonaj analizę luk w systemie i porównaj z czterema komponentami i dwunastoma elementami zwartymi w strukturze ICAO SMS dla zidentyfikowania istniejących i brakujących w organizacji systemów bezpieczeństwa. Wytyczne odnośnie analizy luk w systemie znajdują się w Dodatku 2 do Rozdziału 7.

- W oparciu o wyniki analizy luk w systemie, osoba lub grupa planująca powinna być w stanie przygotować plan wdrożenia SMS z uwzględnieniem:

  — identyfikacji potencjalnych luk w systemie, które mogą utrudnić wdrożenie SMS;
  — strategii odnośnie stwierdzonych luk.

1.3 **Założenia i polityka bezpieczeństwa** (omówiono w Rozdziale 8)

*Polityka bezpieczeństwa*

- Opracuj politykę bezpieczeństwa.

- Doprowadź do podpisania polityki bezpieczeństwa przez Dyrektora Odpowiedzialnego.

- Poinformuj całą organizację o polityce bezpieczeństwa i przekaż, że została przyjęta.

- Opracuj harmonogram przeglądów polityki bezpieczeństwa, aby zapewnić, że nadal jest prawidłowa i odpowiednia dla organizacji.

Przykład oświadczenia dot. polityki bezpieczeństwa można znaleźć w Rozdziale 8.

*Założenia bezpieczeństwa*

- Określ założenia bezpieczeństwa dla SMS poprzez wypracowanie standardów odnośnie poziomu bezpieczeństwa w rozumieniu:

— wskaźników poziomów bezpieczeństwa;
— celów, które mają być osiągnięte przez określone poziomy bezpieczeństwa;
— plany działań.

• Określ wymagania SMS dla podwykonawców:

— określ procedury dla wprowadzenia wymagań SMS do procesów kontraktowych;
— zdefiniuj wymagania SMS w dokumentach przetargowych.

1.4 **Odpowiedzialności i wyznaczanie kluczowego personelu odpowiedzialnego za bezpieczeństwo** (omówiono w Rozdziale 8 niniejszego podręcznika)

*Struktura organizacyjna SMS*

• Powołaj biuro ds. bezpieczeństwa.

• Wyznacz Dyrektora ds. Bezpieczeństwa, który będzie odpowiedzialny za stworzenie i utrzymanie skutecznego SMS i jednocześnie będzie punktem kontaktowym.

• Oceń i ustanów ścieżki komunikacji pomiędzy służbami bezpieczeństwa i Odpowiedzialnym Kierownictwem, Grupą Reagowania ds. bezpieczeństwa (*Safety Action Grou*p (SAG)) i Komisją ds. przeglądu bezpieczeństwa (*Safety Review Board* (SRB)).

• Dopilnuj, aby ścieżki komunikacji było odpowiednie dla wielkości organizacji i złożoności oferowanych usług.

• Powołaj Komisję ds. Przeglądu Bezpieczeństwa (SRB) pod przewodnictwem Dyrektora Odpowiedzialnego.

• Wyznacz do udziału w SRB kierowników, włącznie z kierownikami liniowymi odpowiedzialnymi za obszary funkcjonalne.

• Przypisz SRB odpowiednie elementy strategii.

• Powołaj Grupą Reagowania ds. bezpieczeństwa (*Safety Action Group* (SAG))

• Wyznacz do udziału w SAG kierowników liniowych i przedstawicieli personelu z pierwszej linii.

• Przypisz SRB odpowiednie funkcje taktyczne.

• Udokumentuj wszystkie obowiązki, zakres odpowiedzialności i upoważnienia oraz przekaż tę informację całej organizacji, wraz z definicją poziomów zarządzania mających upoważnienie do podejmowania decyzji związanych z tolerancją ryzyka bezpieczeństwa.

• Opracuj harmonogram spotkań biura/działu służb bezpieczeństwa z SRB i SAG, zgodnie z zapotrzebowaniem.

1.5 **Koordynacja planu reagowania w sytuacji awaryjnej (*Emergency Response Plan* (ERP))** (omówiono w Rozdziale 8)

*Koordynacja wewnętrzna*

• Przejrzyj wytyczne ERP związane z przekazaniem władzy i przypisaniem odpowiedzialności w sytuacji awaryjnej.

• Opracuj procedury współpracy, które muszą być przestrzegane przez personel kluczowy podczas sytuacji awaryjnej i procedury powrotu do operacji standardowych.

*Koordynacja zewnętrzna*

- Zidentyfikuj przedsiębiorstwa zewnętrzne, które będą wzajemnie na siebie oddziaływać w czasie sytuacji awaryjnych.
- Oceń je w odniesieniu do ERP.
- Ustanów koordynację pomiędzy różnymi ERP.
- Wprowadź zasady koordynacji wśród różnych ERP do podręcznika zarządzania systemami bezpieczeństwa organizacji (SMSM).

1.6 **Dokumentacja SMS** (omówiono w Rozdziale 8)

*Dokumentacja SMS*

- Określ mechanizm zbierania i przechowywania rejestrów i dokumentacji specyficznej dla SMS.
- Odnieś się do wszystkich, mających zastosowanie przepisów krajowych i standardów międzynarodowych.
- Opracuj wytyczne dla zarządzania dokumentacją, włącznie z planem wdrożenia SMS i SMSM.

*Plan wdrożenia SMS*

- Wyznacz osobę lub powołaj grupę planowania odpowiedzialną za opracowania planu wdrożenia SMS.
- Zbierz wszystkie dokumenty, które tworzą plan wdrożenia SMS.
- Prowadź regularne spotkania z kierownictwem w celu oceny postępów.
- Przyznaj zasoby (włącznie z czasem na spotkania), odpowiednie dla najbliższych zadań.
- Uwzględnij znaczące elementy planu wdrożenia SMS w planie biznesowym organizacji.
- Zidentyfikuj koszty związane ze szkoleniem i planowaniem koniecznym dla wdrożenia SMS.
- Przydziel odpowiedni czas dla opracowania i uruchomienia planu wdrożenia SMS dla różnych poziomów zarządzania w organizacji.
- Opracuj budżet dla wdrożenia SMS.
- Zatwierdź wstępny budżet dla wdrożenia SMS.
- Przedstaw plan wdrożenia SMS do zatwierdzenia przez kierownictwo.

*Podręcznik systemów zarządzania bezpieczeństwem (SMSM)*

- Przygotuj projekt SMSM, aby poinformować pracowników o polityce bezpieczeństwa organizacji.

- Rozbuduj, przejrzyj i zmień zawartość SMSM (który jest „żywym dokumentem”) wraz ze zmianami w podejściu etapowym.

1.7 **Promocja bezpieczeństwa — Szkolenie** (omówiono w Rozdziale 9)

*Szkolenie z zakresu bezpieczeństwa*

- Przygotuj udokumentowany proces dla zidentyfikowania potrzeb szkoleniowych.
- Przygotuj proces walidacji, który mierzy skuteczność szkolenia.
- Przygotuj szkolenie z zakresu bezpieczeństwa z uwzględnieniem:
  - — szkolenia wstępnego (ogólne bezpieczeństwo), specyficznego dla wykonywanej pracy;
  - — szkolenia wprowadzającego/wstępnego zawierającego SMS, włącznie z czynnikiem ludzkim i czynnikami organizacyjnymi;
  - — szkolenia odświeżającego.
- Określ koszty związane ze szkoleniem.
- Zorganizuj i opracuj harmonogramy odpowiedniego szkolenia dla wszystkich pracowników, zgodnie z indywidualnym zaangażowaniem w SMS.
- Stwórz dla każdego pracownika i kierownika teczkę szkoleniową.

1.8 **Promocja bezpieczeństwa — Wymiana informacji o bezpieczeństwie** (omówiono w Rozdziale 9)

- Określ sposoby przekazywania informacji organizacyjnych dot. Etapu I, włącznie z:
  - — ulotkami, zawiadomieniami i biuletynami bezpieczeństwa;
  - — stronami internetowymi;
  - — wiadomościami e-mail.

1.9 **Czas wdrożenia i produkty końcowe**

Zakładany czas wdrożenia Etapu I wynosi od 1 do 6 miesięcy, w zależności od wielkości organizacji i złożoności świadczonych usług.

**Produkty końcowe**

1) Polityka bezpieczeństwa podpisana przez Dyrektora Odpowiedzialnego.
2) Polityka bezpieczeństwa ogłoszona wszystkim pracownikom.
3) Zakończony opis systemu.
4) Zakończona analiza luk w systemie.
5) Opracowana struktura organizacyjna SMS.
6) Zatwierdzony plan wdrożenia SMS.
7) Przeprowadzone szkolenie w zakresie planowania SMS w etapach.

8) Pierwszy projekt SMSM opublikowany.

9) Wytyczone ścieżki komunikacji.

## 2. ETAP II — REAKTYWNE PROCESY ZARZĄDZANIA BEZPIECZEŃSTWEM

2.1 **Identyfikacja zagrożenia i analiza oparta na procesie reaktywnym** (omówiono w Rozdziałach 3, 4 i 9)

*Identyfikacja zagrożenia*

- Zidentyfikuj wewnętrzne i zewnętrzne źródła, które będą wykorzystane do zbierania reaktywnych informacji na temat zagrożeń.

- Wprowadź podejście strukturalne do reaktywnej identyfikacji zagrożeń.

2.2 **Zarządzanie ryzykiem bezpieczeństwa w oparciu o procesy reaktywne** (omówiono w Rozdziałach 5 i 9)

*Ocena ryzyka bezpieczeństwa*

- Opracuj i wprowadź do operacyjnego środowiska organizacji matrycę ryzyka bezpieczeństwa.

- Opracuj instrukcje dla matrycy ryzyka bezpieczeństwa i włącz je do programu szkolenia.

2.3 **Szkolenie** (omówiono w Rozdziale 9)

- Opracuj program szkolenia z zakresu bezpieczeństwa dla personelu liniowego, dyrektorów i kierowników na temat:

  — odpowiednich elementów planu wdrażania SMS;
  — identyfikacji zagrożenia i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne (personel liniowy szkolony jest w identyfikowaniu i meldowaniu o zaistniałych zagrożeniach, a kierownicy są szkoleni w zakresie zarządzania zagrożeniem i ryzykiem bezpieczeństwa);
  — druk/wzór zgłoszenia zagrożenia.

2.4 **Dokumentacja procesów reaktywnych** (omówiono w Rozdziałach 4 i 9)

- Stwórz archiwum bezpieczeństwa.

- Włącz informację o reaktywnych procesach zarządzania ryzykiem bezpieczeństwa do SMSM. (Informacja dotycząca reaktywnych procesów zarządzania ryzykiem bezpieczeństwa będzie wykorzystana w późniejszym etapie do określenia wskaźników poziomu bezpieczeństwa i ich celów.)
- Przygotuj wymagania do identyfikacji zagrożenia i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy reaktywne, właściwe dla dokumentacji przetargowej dla kontrahentów i, jeżeli jest to wymagane, poinformuj o tym w formie pisemnej kontrahentów i podwykonawców.

2.5 **Promocja bezpieczeństwa — Wymiana informacji o bezpieczeństwie** (omówiono w Rozdziale 9)

- Określ sposoby przekazywania informacji organizacyjnych dot. Etapu II:

  — ulotki, zawiadomienia i biuletyny bezpieczeństwa;
  — strony internetowe;
  — e-mail.

2.6 **Czas wdrożenia i produkty końcowe**

Zakładany czas wdrożenia Etapu II wynosi od 9 do 12 miesięcy, w zależności od wielkości organizacji i złożoności świadczonych usług.

***Produkty końcowe***

1) Stworzone archiwum publikacji dotyczących bezpieczeństwa („archiwum bezpieczeństwa").

2) Wdrożone reaktywne procesy zarządzania bezpieczeństwem.

3) Ukończone szkolenie w zakresie elementów planu wdrożenia SMS i zarządzania ryzykiem bezpieczeństwa.

4) Rozpowszechniona w organizacji krytyczna informacja związana z danymi bezpieczeństwa pozyskiwanymi z procesów reaktywnych.

**3. ETAP III — PROAKTYWNE I PROGNOZUJĄCE PROCESY ZARZĄDZANIA BEZPIECZEŃSTWEM**

3.1 **Identyfikacja zagrożenia i analiza oparta na procesie proaktywnym i prognozującym** (omówiono w Rozdziałach 3, 4 i 9)

*Identyfikacja zagrożenia*

- Zidentyfikuj wewnętrzne i zewnętrzne źródła, które będą wykorzystane do zbierania proaktywnych i prognozujących informacji na temat zagrożeń.

- Wprowadź podejście strukturalne do proaktywnej i prognozującej identyfikacji zagrożeń.

3.2 **Zarządzanie ryzykiem bezpieczeństwa w oparciu o procesy proaktywne i prognozujące** (omówiono w Rozdziałach 5 i 9)

*Ocena ryzyka bezpieczeństwa*

- Opracuj i wprowadź do operacyjnego środowiska organizacji matrycę ryzyka bezpieczeństwa.

- Opracuj instrukcje dla matrycy ryzyka bezpieczeństwa i włącz je do programu szkolenia.

3.3 **Szkolenie** (omówiono w Rozdziale 9)

- Przeprowadź szkolenie dla pracowników wydziału ds. bezpieczeństwa na temat proaktywnych i prognozujących środków zbierania danych związanych z bezpieczeństwem.

- Przeprowadź szkolenie dla kierowników i pracowników liniowych w zakresie procesów proaktywnych i prognozujących.

- Opracuj program szkolenia z zakresu bezpieczeństwa dla personelu liniowego, dyrektorów i kierowników na temat:

  — odpowiednich elementów planu wdrażania SMS;
  — identyfikacji zagrożenia i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy proaktywne i prognozujące (personel liniowy szkolony jest w identyfikowaniu i meldowaniu o zagrożeniach w oparciu o wywoływane mniej poważne zdarzenia lub podczas normalnych operacji w rzeczywistym czasie, a kierownicy są szkoleni w zakresie zarządzania zagrożeniem i ryzykiem bezpieczeństwa w oparciu o procesy proaktywne i prognozujące).

3.4 **Dokumentacja procesów proaktywnych i prognozujących** (omówiono w Rozdziałach 4 i 9)

- Przechowuj w „archiwum bezpieczeństwa" informację związaną z zarządzaniem ryzykiem bezpieczeństwa, pozyskaną w oparciu o procesy proaktywne i prognozujące.

- Włącz do SMSM informację o proaktywnych i prognozujących procesach zarządzania ryzykiem bezpieczeństwa.

- Opracuj wskaźniki i założenia dla poziomów bezpieczeństwa.

- Przygotuj wymagania dla identyfikacji zagrożenia i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy proaktywne i prognozujące, właściwe dla dokumentacji przetargowej dla kontrahentów i jeżeli jest to wymagane, poinformuj o tym w formie pisemnej kontrahentów i podwykonawców .

3.5 **Promocja bezpieczeństwa — Wymiana informacji o bezpieczeństwie**
(omówiono w Rozdziale 9)

- Określ sposoby przekazywania informacji organizacyjnych dot. Etapu III:

  — ulotki, zawiadomienia i biuletyny bezpieczeństwa;
  — strony internetowe;
  — e-mail.

3.6 **Czas wdrożenia i produkty końcowe**

Zakładany czas wdrożenia Etapu III wynosi od 12 do 16 miesięcy w zależności od wielkości organizacji i złożoności świadczonych usług.

***Produkty końcowe***

1) Określony wstępny okres sprawdzania proaktywnych i prognozujących środków zbierania identyfikacji zagrożeń.

2) Wdrożone proaktywne i prognozujące procesy zarządzania bezpieczeństwem.

3) Ukończone szkolenie w zakresie elementów planu wdrożenia SMS i zarządzania ryzykiem bezpieczeństwa w oparciu o procesy proaktywne i prognozujące.

4) Opracowane wskaźniki i założenia dla poziomów bezpieczeństwa.

5) Rozpowszechniona w organizacji krytyczna informacja związana z danymi bezpieczeństwa pozyskiwanymi z procesów reaktywnych, proaktywnych i prognozujących.

## 4. ETAP IV — ZAPEWNIENIE BEZPIECZEŃSTWA OPERACYJNEGO

4.1 **Stan bezpieczeństwa SMS** (omówiony w Rozdziale 9)

- Określ wskaźniki dla poziomów bezpieczeństwa.
- Określ założenia dla poziomów bezpieczeństwa.
- Opracuj plany działań.
- Zdefiniuj wskaźniki wiarygodności, dostępności i/lub dokładności w odniesieniu do planów działania, zgodnie z potrzebami.
- Uzgodnij z nadzorem państwowym sposoby/narzędzia pomiaru poziomu bezpieczeństwa.

4.2 **Monitorowanie i analiza poziomu bezpieczeństwa** (omówiony w Rozdziale 9)

- Zdefiniuj i opracuj źródła informacji dot. monitorowania i analizy poziomu bezpieczeństwa.

4.3 **Zarządzanie zmianami** (omówiono w Rozdziale 9)

- Stwórz formalny proces zarządzania zmianami, który uwzględnia:
  - — krytyczność systemów i czynności;
  - — stabilność systemów i środowisk operacyjnych;
  - — dotychczasowe działania.
- Zidentyfikuj zmiany, które mogą mieć wpływ na ustanowione procesy, procedury, produkty i usługi.
- Przed wprowadzeniem zmian zidentyfikuj warunki zapewniające odpowiedni poziom bezpieczeństwa.

4.4 **Ciągłe usprawnianie SMS** (omówiono w Rozdziale 9)

- Opracuj zasady ocen wewnętrznych i zapewnij niezależność od ocenianych procesów technicznych.
- Zdefiniuj proces audytu wewnętrznego.
- Zdefiniuj proces audytu zewnętrznego.

- Określ harmonogram proaktywnej oceny obiektów, wyposażenia, dokumentacji i procedur do wykonania podczas audytów i analiz.

- Określ harmonogram proaktywnej oceny pracy pracownika.

- Przygotuj dokumentację związaną z zapewnieniem bezpieczeństwa operacyjnego.

4.5 **Szkolenie** (omówiono w Rozdziale 9)

- Przygotuj szkolenie związane z zapewnieniem bezpieczeństwa operacyjnego dla pracowników zaangażowanych w ten etap.

4.6 **Promocja bezpieczeństwa — Wymiana informacji o bezpieczeństwie** (omówiono w Rozdziale 9)

- Określ sposoby przekazywania informacji organizacyjnych dot. Etapu IV:

  — ulotki, zawiadomienia i biuletyny bezpieczeństwa;
  — strony inetrnetowe;
  — e-mail.

4.7 **Czas wdrożenia i produkty końcowe**

Zakładany czas wdrożenia Etapu IV wynosi od 9 do 12 miesięcy, w zależności od wielkości organizacji i złożoności świadczonych usług.

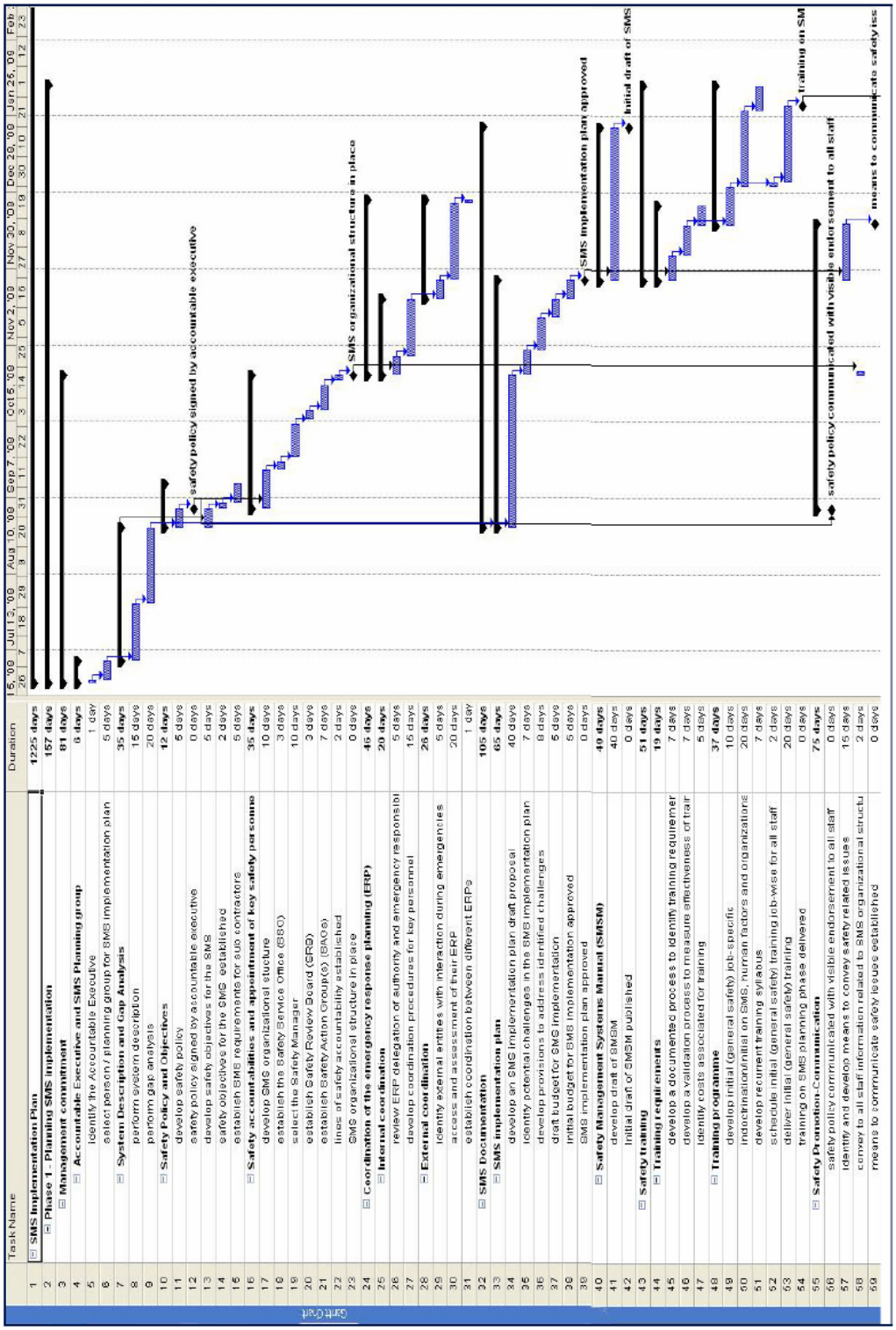
***Produkty końcowe***

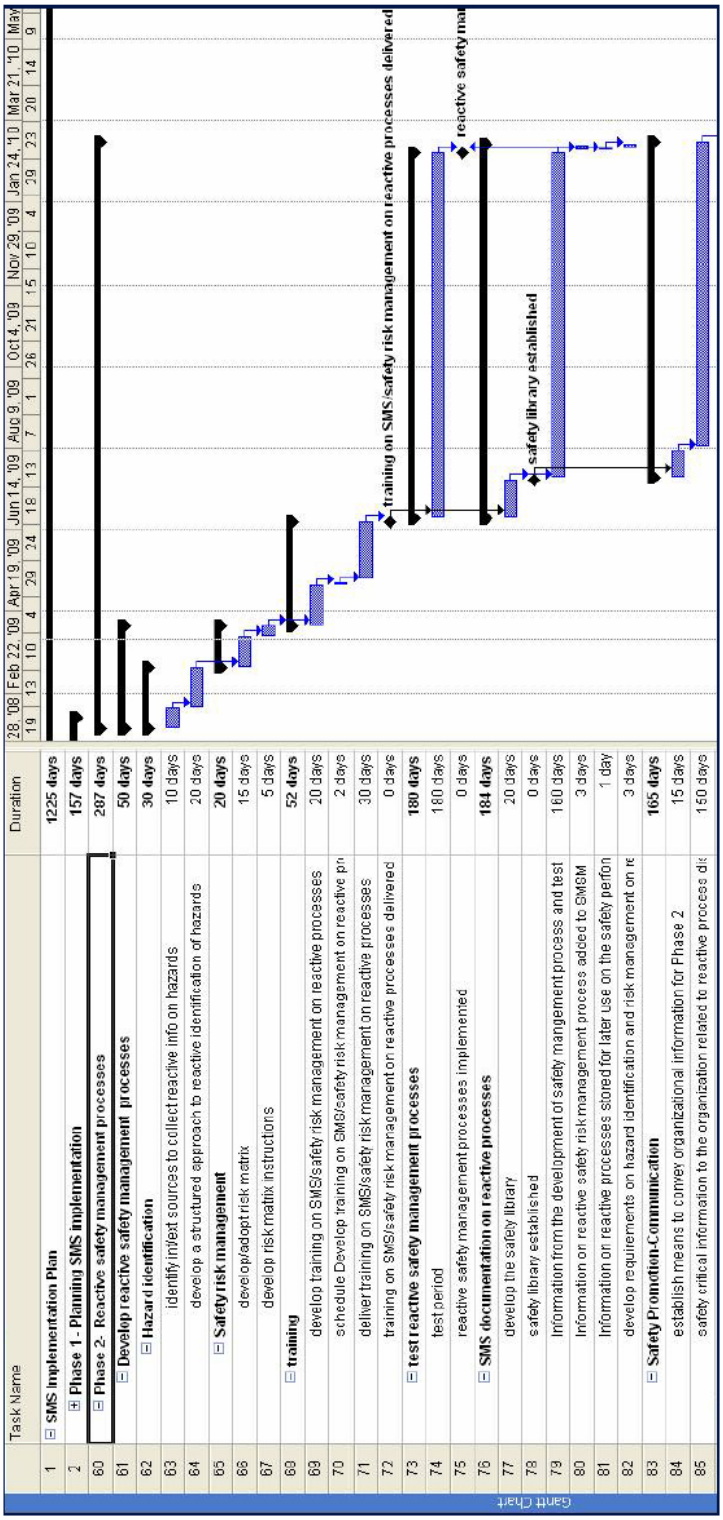
1) Wskaźniki i założenia dla poziomów bezpieczeństwa są uzgodnione z państwową władzą nadzorującą.

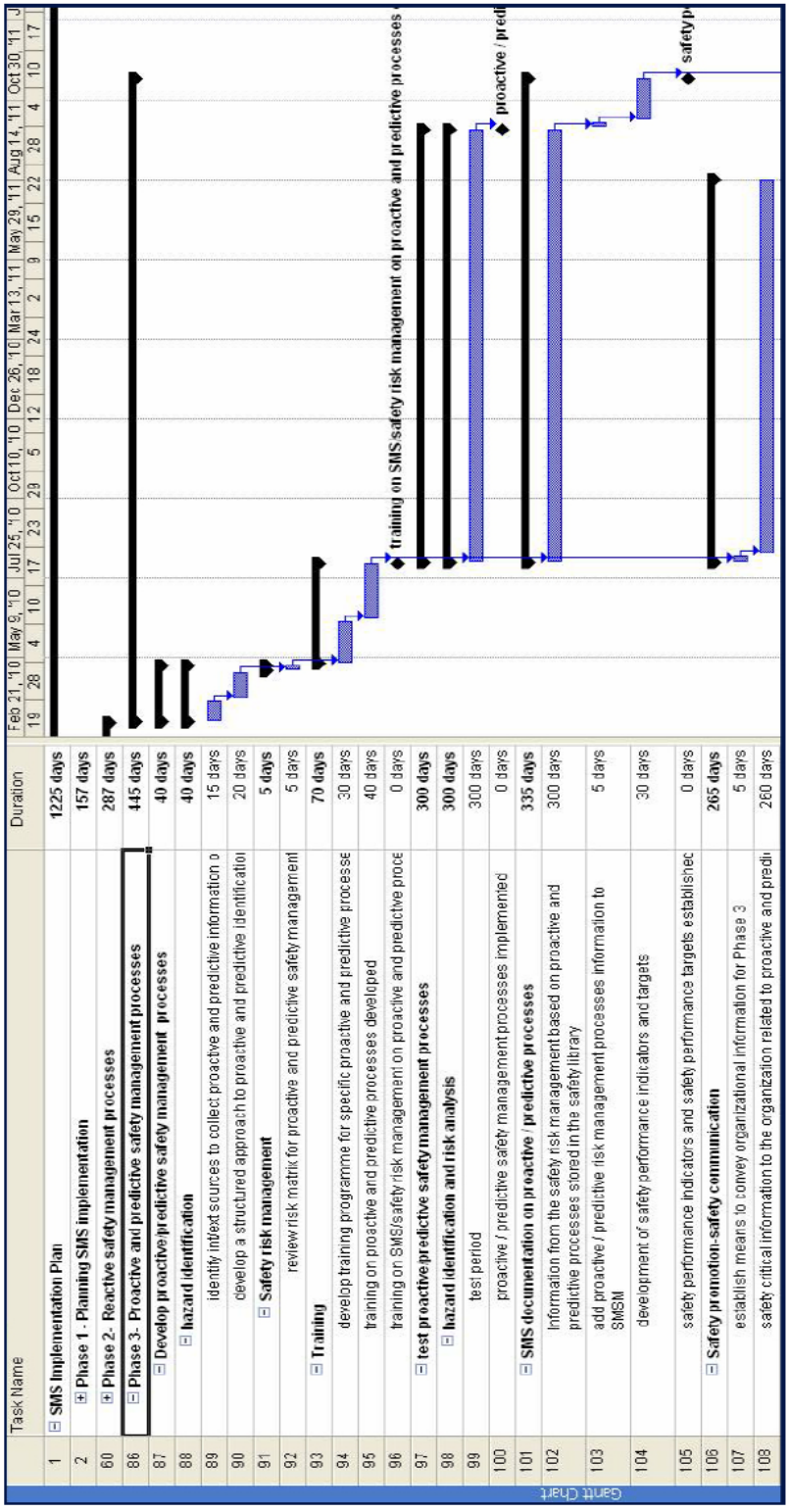
2) Szkolenie z zakresu zapewnienia bezpieczeństwa dla personelu operacyjnego, dyrektorów i kierowników zostało zakończone.

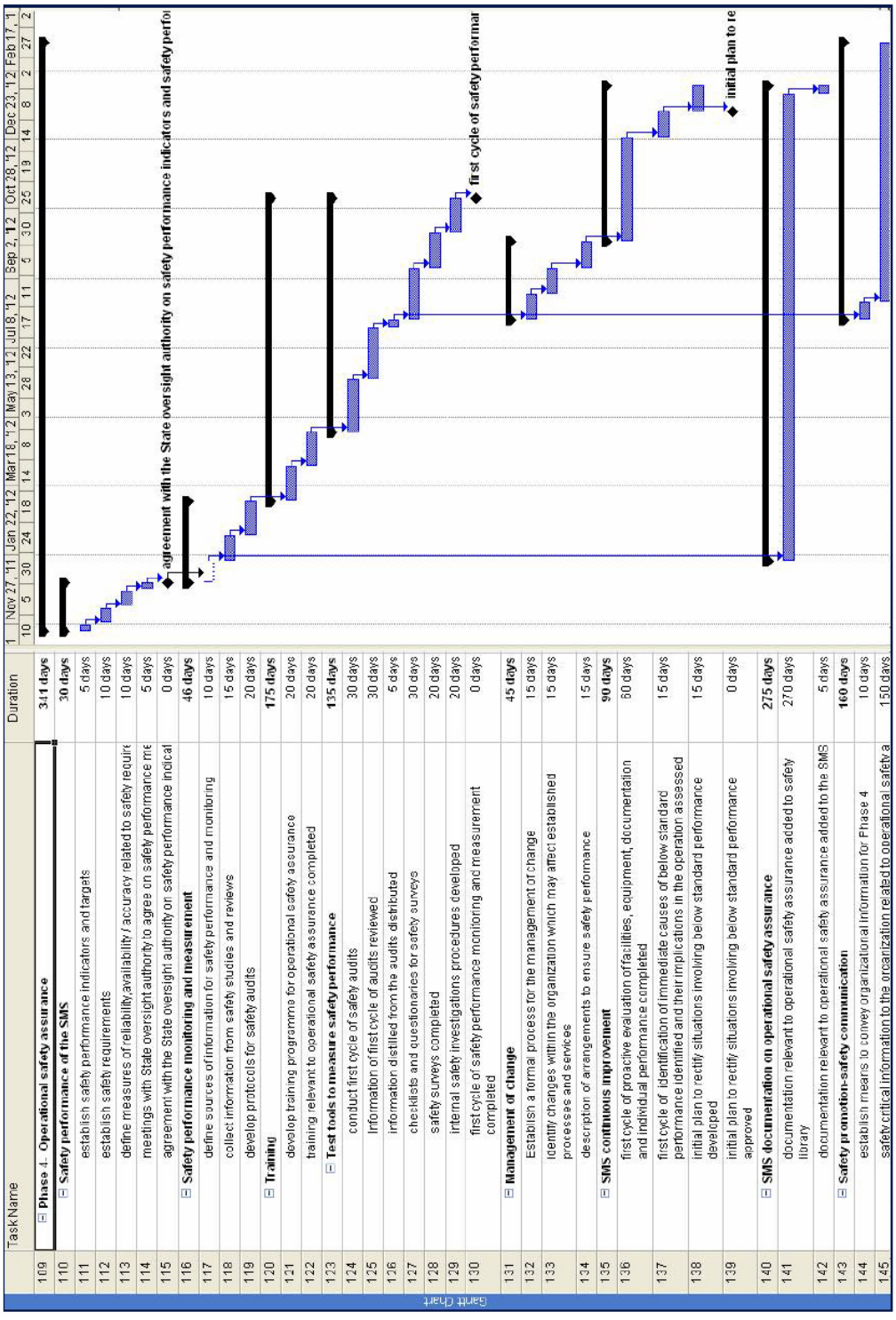
3) Dokumentacja odpowiednia dla zapewnienia bezpieczeństwa operacyjnego znajduje się w ”archiwum bezpieczeństwa”.

**Wykres Gantt'a – Wdrożenie planu SMS**




Gantt Chart
Task Name
Duration
1 SMS implementation Plan 1225 days
2 Phase 1 - Planning SMS implementation 157 days
60 Phase 2- Reactive safety management processes 287 days
61 Develop reactive safety management processes 50 days
62 Hazard identification 30 days
63 identify/collect sources to collect reactive info on hazards 10 days
64 develop a structured approach to reactive identification of hazards 20 days
65 Safety risk management 20 days
66 develop/adopt risk matrix 15 days
67 develop risk matrix instructions 5 days
68 training 52 days
69 develop training on SMS/safety risk management on reactive processes 20 days
70 schedule Develop training on SMS/safety risk management on reactive pr 2 days
71 deliver training on SMS/safety risk management on reactive processes 30 days
72 training on SMS/safety risk management on reactive processes delivered 0 days
73 test reactive safety management processes 180 days
74 test period 180 days
75 reactive safety management processes implemented 0 days
76 SMS documentation on reactive processes 184 days
77 develop the safety library 20 days
78 safety library established 0 days
79 Information from the development of safety mangement process and test 160 days
80 Information on reactive safety risk management process added to SMSM 3 days
81 Information on reactive processes stored for later use on the safety perfon 1 day
82 develop requirements on hazard identification and risk management on re 3 days
83 Safety Promotion-Communication 165 days
84 establish means to convey organizational information for Phase 2 15 days
85 safety critical information to the organization related to reactive process dis 150 days
28 '08 Feb 22 '09 Apr 19 '09 Jun 14 '09 Aug 9 '09 Oct 4 '09 Nov 29 '09 Jan 24 '10 Mar 21 '10 May
training on SMS/safety risk management on reactive processes delivered
safety library established
reactive safety ma


Task Name
Duration
Feb 21, '10
May 9, '10
Jul 25, '10
Oct 10, '10
Dec 26, '10
Mar 13, '11
May 29, '11
Aug 14, '11
Oct 30, '11
1 SMS Implementation Plan 1225 days
2 Phase 1 - Planning SMS implementation 157 days
60 Phase 2- Reactive safety management processes 287 days
86 Phase 3- Proactive and predictive safety management processes 445 days
87 Develop proactive/predictive safety management processes 40 days
88 hazard identification 40 days
89 identify int/ext sources to collect proactive and predictive information o 15 days
90 develop a structured approach to proactive and predictive identificatio 20 days
91 Safety risk management 5 days
92 review risk matrix for proactive and predictive safety management 5 days
93 Training 70 days
94 develop training programme for specific proactive and predictive processe 30 days
95 training on proactive and predictive processes developed 40 days
96 training on SMS/safety risk management on proactive and predictive proce 0 days
97 test proactive/predictive safety management processes 300 days
98 hazard identification and risk analysis 300 days
99 test period 300 days
100 proactive / predictive safety management processes implemented 0 days
101 SMS documentation on proactive / predictive processes 335 days
102 Information from the safety risk management based on proactive and predictive processes stored in the safety library 300 days
103 add proactive / predictive risk management processes information to SMSM 5 days
104 development of safety performance indicators and targets 30 days
105 safety performance indicators and safety performance targets established 0 days
106 Safety promotion-safety communication 265 days
107 establish means to convey organizational information for Phase 3 5 days
108 safety critical information to the organization related to proactive and predi 260 days
training on SMS safety risk management on proactive and predictive processes
proactive / predi
safety p
Gantt Chart


Gantt Chart
Task Name
Duration
Phase 4. Operational safety assurance 344 days
Safety performance of the SMS 30 days
establish safety performance indicators and targets 5 days
establish safety requirements 10 days
define measures of reliability,availability / accuracy related to safety requir 10 days
meetings with State oversight authority to agree on safety performance me 5 days
agreement with the State oversight authority on safety performance indicat 0 days
Safety performance monitoring and measurement 46 days
define sources of information for safety performance and monitoring 10 days
collect information from safety studies and reviews 15 days
develop protocols for safety audits 20 days
Training 175 days
develop training programme for operational safety assurance 20 days
training relevant to operational safety assurance completed 20 days
Test tools to measure safety performance 135 days
conduct first cycle of safety audits 30 days
Information of first cycle of audits reviewed 30 days
information distilled from the audits distributed 5 days
checklists and questionaries for safety surveys 30 days
safety surveys completed 20 days
internal safety investigations procedures developed 20 days
first cycle of safety performance monitoring and measurement completed 0 days
Management of change 45 days
Establish a formal process for the management of change 15 days
identify changes within the organization which may affect established processes and services 15 days
description of arrangements to ensure safety performance 15 days
SMS continuous improvement 90 days
first cycle of proactive evaluation of facilities, equipment, documentation and individual performance completed 60 days
first cycle of identification of immediate causes of below standard performance identified and their implications in the operation assessed 15 days
initial plan to rectify situations involving below standard performance developed 15 days
initial plan to rectify situations involving below standard performance approved 0 days
SMS documentation on operational safety assurance 275 days
documentation relevant to operational safety assurance added to safety library 270 days
documentation relevant to operational safety assurance added to the SMS 5 days
Safety promotion-safety communication 160 days
establish means to convey organizational information for Phase 4 10 days
safety critical information to the organization related to operational safety a 150 days
agreement with the State oversight authority on safety performance indicators and safety perfo
first cycle of safety performar
initial plan to re
Nov 27, '11
Jan 22, '12
Mar 18, '12
May 13, '12
Jul 8, '12
Sep 2, '12
Oct 28, '12
Dec 23, '12
Feb 17, '1

# Rozdział 11

# KRAJOWY PROGRAM BEZPIECZEŃSTWA (SSP)

## 11.1 CELE I ZAWARTOŚĆ

Niniejszy rozdział wprowadza podstawy do opracowania i wdrożenia krajowego programu bezpieczeństwa (SSP) łączącego elementy zarówno normatywnego, jak i opartego na wynikach (performance-based) podejścia do zarządzania bezpieczeństwem. Rozdział ten omawia również znaczenie realistycznego wdrożenia SSP jako warunku koniecznego do wdrożenia SMS przez podmioty prowadzące działalność lotniczą. Niniejszy rozdział zawiera następujące tematy:

a) składniki i elementy SSP;

b) podstawy SSP wg ICAO;

c) opracowanie SSP;

d) wdrażanie SSP;

e) rola SSP we wspieraniu wdrażania SMS.

## 11.2 SKŁADNIKI I ELEMENTY SSP

11.2.1 SSP jest systemem zarządzania pozwalającym państwom zarządzać bezpieczeństwem. Wdrażanie SSP musi odpowiadać wielkości i złożoności systemu lotnictwa w danym państwie i może wymagać koordynacji pomiędzy wieloma władzami odpowiedzialnymi za poszczególne funkcje państwa związane z lotnictwem cywilnym.

11.2.2 Istnieją cztery składniki SSP, odzwierciedlające dwa kluczowe obszary działania operacyjnego SSP oraz rozwiązania organizacyjne niezbędne przy realizacji działań w tych obszarach.
Czterema składnikami SSP są:

a) polityka i cele państwa w zakresie bezpieczeństwa;

b) zarządzanie ryzykiem przez państwo;

c) zapewnianie bezpieczeństwa przez państwo;

d) promowanie bezpieczeństwa przez państwo.

11.2.3 Z punktu widzenia strategii interwencji i zapobiegania w dziedzinie bezpieczeństwa, dwoma kluczowymi obszarami działania operacyjnego SSP są: zarządzanie ryzykiem i zapewnianie bezpieczeństwa przez państwo. Te kluczowe obszary działania operacyjnego funkcjonują w ramach polityki i celów państwa w dziedzinie bezpieczeństwa i wspierane są przez promowanie bezpieczeństwa przez państwo. Większość odpowiednich składników SMS przedstawionych w rozdziale 8, 8.2 i 8.3 ma również zastosowanie do SSP. Jednakże istnieje jeden wyjątek: choć wprawdzie w SSP proces badania wypadków i poważnych incydentów jest formalnie uważany za element polityki i celów państwa w zakresie bezpieczeństwa, to jest on także kluczowym obszarem działania operacyjnego, który przyczynia się do zbierania, analizy i wymiany danych dotyczących bezpieczeństwa oraz identyfikowania obszarów nadzoru wymagających większej uwagi (zapewnianie bezpieczeństwa przez państwo).

11.2.4 Cztery składniki omówione w punkcie 11.2.2 stanowią podstawy, na których opiera się SSP, gdyż reprezentują cztery zazębiające się procesy zarządzania bezpieczeństwem leżące u podstaw właściwego systemu zarządzania (SSP). Każdy składnik dzieli się na elementy obejmujące określone podprocesy, działania lub narzędzia, które system bezpieczeństwa musi uruchamiać lub wykorzystywać w celu zarządzania bezpieczeństwem w sposób łączący podejście normatywne (*prescriptive*) z opartym na wynikach (*performance-based*), a także wspiera wdrażanie SMS przez podmioty lotnicze.

11.2.5 Składnik dotyczący polityki i celów państwa w zakresie bezpieczeństwa składa się z czterech elementów:

a) obowiązujące w państwie przepisy dotyczące bezpieczeństwa;

b) określenie w ramach państwa zakresów odpowiedzialności za bezpieczeństwo;

c) badanie wypadków i incydentów;

d) polityka zapewniania przestrzegania przepisów.

11.2.6 Składnik dotyczący zarządzania ryzykiem przez państwo składa się z dwóch elementów:

a) wymagania dotyczące SMS podmiotów lotniczych;

b) uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.

11.2.7 Składnik dotyczący zapewnienia bezpieczeństwa przez państwo składa się z trzech elementów:

a) nadzór nad bezpieczeństwem;

b) zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa;

c) ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach.

11.2.8 Składnik dotyczący promowania bezpieczeństwa przez państwo składa się z dwóch elementów:

a) wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa;

b) zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

*Uwaga.— W kontekście SSP pojęcie „podmiot lotniczy" odnosi się do każdej organizacji dostarczającej usługi lotnicze. Pojęcie to obejmuje zatwierdzone organizacje szkoleniowe wystawione na zagrożenia podczas świadczenia usług, użytkowników statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projektowanie i/lub produkcję statków powietrznych, dostawców usług ruchu lotniczego i certyfikowane lotniska.*

### 11.3 PODSTAWY SSP WG ICAO

*Uwaga.— Szczegółowe informacje na temat podstaw SSP wg ICAO zawarte są w Dodatku 1 do niniejszego rozdziału.*

11.3.1 Cztery składniki w połączeniu z elementami omówionymi w części 11.2 stanowią podstawy SSP wg ICAO, pomyślane jako przewodnik do stworzenia, wdrożenia i funkcjonowania SSP:

1. Polityka i cele państwa w zakresie bezpieczeństwa

   1.1 obowiązujące w państwie przepisy dotyczące bezpieczeństwa;

   1.2 określenie w ramach państwa zakresów odpowiedzialności za bezpieczeństwo;

   1.3 badanie wypadków i incydentów;

   1.4 polityka zapewniania przestrzegania przepisów.

2. Zarządzanie ryzykiem przez państwo

   2.1 wymagania dotyczące SMS podmiotów lotniczych;

   2.2 uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.

3. Zapewnianie bezpieczeństwa przez państwo

   3.1 nadzór nad bezpieczeństwem;

   3.2 zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa;

   3.3 ukierunkowanie nadzoru dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach.

4. Promowanie bezpieczeństwa przez państwo

   4.1 wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa;

   4.2 zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

11.3.2 Podstawy SSP wprowadzone w niniejszym rozdziale i podstawy systemu zarządzania bezpieczeństwem (SMS) z rozdziału 8 powinny być postrzegane jako uzupełniające się, chociaż odrębne.

### 11.4 OPRACOWANIE SSP

11.4.1 Proponuje się, aby państwa tworzyły SSP wokół czterech składników i jedenastu elementów podstaw SSP wg ICAO.

11.4.2 ***Polityka i cele państwa w dziedzinie bezpieczeństwa.*** Opis tego, jak państwo będzie nadzorować zarządzanie bezpieczeństwem w działalności lotniczej na swoim terytorium. Obejmuje to zdefiniowanie wymagań i zakresów odpowiedzialności różnych struktur państwa w odniesieniu do SSP oraz akceptowalnego poziomu bezpieczeństwa (*ALoS*), który ma być osiągnięty w ramach SSP.

11.4.3 Trzy składniki SSP omówione w następnych punktach mogą być skutecznie wdrożone jedynie w ogólnych ramach odpowiedzialności w różnych zakresach i na różnych poziomach. Te ogólne ramy stają się „parasolem ochronnym” dla zarządzania ryzykiem, zapewniania bezpieczeństwa i promowania bezpieczeństwa przez państwo. Składnik dotyczący polityki i celów państwa w zakresie bezpieczeństwa zapewnia kierownictwu i pracownikom klarowne dokumenty programowe, procedury, instrumenty zarządzania, dokumentowania i procesy korygujące, które umożliwiają działania władz lotniczych w dziedzinie zarządzania bezpieczeństwem. Ten składnik jest również kluczowy, jeśli chodzi o budowę zaufania w zdolność państwa do przewodzenia w dziedzinie bezpieczeństwa w coraz bardziej złożonym i stale zmieniającym się systemie transportu lotniczego. Głównym działaniem w ramach tego składnika jest opracowanie polityki państwa w dziedzinie bezpieczeństwa. Dodatek 2 do niniejszego rozdziału zawiera wytyczne do przygotowania dokumentu programowego polityki państwa w zakresie bezpieczeństwa.

11.4.4 ***Zarządzanie ryzykiem przez państwo.*** Opis tego, jak państwo będzie identyfikować zagrożenia i oceniać ryzyka dla bezpieczeństwa wynikające z zagrożeń w operacjach lotniczych na terytorium państwa. Obejmuje to również ustanowienie mechanizmów (przepisów) określających, jak państwo ma zarządzać bezpieczeństwem, przepisów określających funkcjonowanie SMS podmiotów lotniczych oraz uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.

11.4.5 Zasady zarządzania bezpieczeństwem mają wpływ na większość działań państwowej władzy lotnictwa cywilnego, poczynając od stanowienia prawa. Zamiast skupiać się wyłącznie na przyczynach ostatniego wypadku, prawo stanowione w ramach SSP opiera się na kompleksowej analizie systemu lotnictwa w państwie. Regulacje oparte są na zidentyfikowanych zagrożeniach oraz analizie ryzyka związanego z konsekwencjami zagrożeń. Regulacje implementowane do SMS podmiotów lotniczych stanowią podstawę kontroli ryzyka.

11.4.6 ***Zapewnianie bezpieczeństwa przez państwo.*** Opis tego jak państwo zapewni, że zarządzanie bezpieczeństwem na terytorium państwa oraz funkcjonowanie SMS podmiotów lotniczych są zgodne z ustalonymi zasadami (zgodność z przepisami), jak zostaną osiągnięte realistyczne, akceptowalne poziomy bezpieczeństwa poprzez kombinację pomiaru poziomu bezpieczeństwa w państwie i przez podmioty lotnicze, a także jak wykazywane będą rzeczywiste wskaźniki bezpieczeństwa w SMS podmiotów lotniczych (*safety performance measurement* – pomiar rzeczywistego poziomu bezpieczeństwa). Obejmuje to również ustanowienie rozwiązań (nadzór, inspekcje, audyty, analiza danych etc.) niezbędnych do weryfikowania przestrzegania przepisów i pomiaru bezpieczeństwa w działalności.

11.4.7 ***Nadzór w ramach SSP.*** Działania nadzorcze w ramach SSP, poza ustanawianiem norm, są poparte analizami. Priorytety przy alokacji zasobów władzy lotniczej państwa oparte są na ryzykach wynikających z konsekwencji zagrożeń dla bezpieczeństwa wskazanych poprzez analizy. Certyfikacja i bieżące decyzje dotyczące bezpieczeństwa operacyjnego oparte są na ocenie funkcjonowania procesów, produktów i usług danego podmiotu. Na podstawie regulacji dotyczących określonych zagrożeń, decyzje w sprawie zatwierdzenia SMS operatorów oparte są na tym czy SMS danego podmiotu obejmuje zagrożenia określone w regulacjach dotyczących konkretnego środowiska operacyjnego podmiotu. Procesy w ramach zapewniania bezpieczeństwa przez państwo prowadzone są w celu zapewnienia wiarygodności zdolności podmiotów lotniczych do zarządzania bezpieczeństwem poprzez ocenę SMS.

11.4.8 ***Promowanie bezpieczeństwa przez państwo.*** Opis działań podejmowanych przez państwo w celu zapewnienia komunikacji i upowszechniania informacji dotyczących bezpieczeństwa. W SSP jest to promowanie dwutorowe, zarówno wewnątrz instytucji państwa odpowiedzialnych za lotnictwo, jak i pośród podmiotów lotniczych nadzorowanych przez państwo. Obejmuje to ustanowienie rozwiązań koniecznych do zapewnienia szkolenia i komunikowania informacji dotyczących bezpieczeństwa.

11.4.9 Żadne z zagadnień opisanych powyżej, nie zmienia roli państwa i jego struktur odpowiedzialnych za lotnictwo w zakresie ustanawiania regulacji i standardów obowiązujących w państwie; nie zmienia to też konieczności posiadania przez pracowników państwowych wysokiego poziomu wiedzy i umiejętności. Wręcz przeciwnie, wymaga to dodatkowych umiejętności w dziedzinach takich jak analiza ryzyka, ewaluacja systemowa i ocena systemów zarządzania, a także w zakresie wielu nowych technologii, kluczowych dla osiągnięcia przez sektor lotniczy założonych celów produkcyjnych. Dlatego też państwo ma obowiązek zapewniania tych kompetencji poprzez szkolenie, rekrutację i zarządzanie zasobami ludzkimi.

11.4.10 Podczas tworzenia SSP, zasady zarządzania bezpieczeństwem stanowią wspólną platformę pojęciową dla równoległego opracowywania SSP przez państwo i SMS przez podmioty lotnicze. Oparty o zasady zarządzania bezpieczeństwem SSP wypełnia lukę, która mogłaby się pojawić pomiędzy wewnętrznymi i zewnętrznymi procesami zarządzania bezpieczeństwem w instytucjach państwa odpowiedzialnych za lotnictwo i wewnętrznymi procesami podmiotów lotniczych (patrz wykres 11-1). W ramach SSP Państwo ustala wymagania dotyczące SMS podmiotów lotniczych, zobowiązując je do zademonstrowania z góry zdolności do zarządzania bezpieczeństwem, zamiast oczekiwania na wypadki, incydenty bądź nieprzestrzeganie standardów bezpieczeństwa. Pozwala to zarówno państwu, jak i podmiotom lotniczym z wyprzedzeniem reagować na ryzyka. Wymagania dotyczące SMS w ramach SSP stanowią również ustrukturyzowane ramy dla skuteczniejszej interakcji pomiędzy państwem a podmiotami lotniczymi w zakresie rozwiązywania problemów związanych z bezpieczeństwem. W ten sposób powiązana, interaktywna natura SSP i SMS daje konkretne rezultaty.

## 11.5 WDRAŻANIE SSP

11.5.1 We wdrażaniu SSP pomaga identyfikacja procesów związanych z każdym z czterech składników SSP omówionych w poprzednich akapitach. Procesy te mogą być wtedy przekształcone w wyraźne elementy składników SSP, a podobnie jak w przypadku podstaw SMS omówionych w rozdziale 8, połączenie składników i elementów tworzy podstawowe ramy SSP. Ramy takie stanowią zasadniczy przewodnik wdrażania SSP. ICAO opracowała wytyczne do tworzenia SSP, aby ułatwić ten proces, a podstawy SSP wg ICAO zawarte są w Dodatku 2 do niniejszego rozdziału. Dodatek 5 do niniejszego rozdziału zawiera wytyczne do planu wdrażania SSP.

11.5.2 Przykład SSP opracowanego przez państwo, Krajowy program bezpieczeństwa Zjednoczonego Królestwa opublikowany jako UK Civil Aviation Publication (CAP) 784, jest dostępny na stronie CAA UK: www.caa.co.uk.

### 11.6 ROLA SSP WE WSPIERANIU WDRAŻANIA SMS

11.6.1 Jednym z celów SSP jest stworzenie warunków sprzyjających wdrażaniu SMS przez podmioty lotnicze. SMS podmiotów lotniczych nie mogą skutecznie funkcjonować w próżni regulacyjnej czy w środowisku zorientowanym wyłącznie na przestrzeganie przepisów. W takim środowisku podmioty lotnicze wdrożą, a władze ocenią jedynie fasadę SMS. SMS może działać prawidłowo jedynie w korzystnych warunkach stworzonych przez SSP. SSP jest więc podstawowym czynnikiem sprzyjającym wdrażaniu efektywnych SMS przez podmioty lotnicze. Dlatego też w ramach ogólnego wdrażania SSP omówionego w Dodatku 5, cztery kroki mają na celu wsparcie wdrażania SMS przez podmioty lotnicze, dwa ogólnie i dwa konkretnie.


**Rysunek 11-1. SSP wypełnia lukę pomiędzy procesami bezpieczeństwa Państwa i podmiotów lotniczych**

11.6.2 Ogólnie pierwszym krokiem do podjęcia przez państwo przy wdrażaniu SSP jest przeprowadzenie analizy luk w celu ustalenia istnienia i stopnia dojrzałości elementów SSP w państwie. Przykład analizy luk zawarty jest w Dodatku 3 do niniejszego rozdziału. W następstwie analizy luk państwo jest w stanie opracować projekty ustaw oraz regulacji operacyjnych określających funkcjonowanie SSP. W tym zawierają się również wymagania dotyczące SMS podmiotów lotniczych.

11.6.3 Wczesnym etapem wdrażania SSP jest opracowanie programu szkolenia personelu władz Państwowych. Program szkolenia powinien mieć dwa zasadnicze cele. Pierwszym celem jest dostarczenie wiedzy o koncepcji zarządzania bezpieczeństwem, w tym SARPs ICAO zawartych w Załącznikach 1, 6, 8, 11, 13 i 14 oraz odpowiednich wytycznych. Ten aspekt szkolenia dotyczy ogólnie SSP. Drugim celem jest przekazanie wiedzy umożliwiającej zatwierdzanie i nadzór nad wdrażaniem głównych składników SMS, zgodnie z przepisami krajowymi i właściwymi SARPs ICAO. Ten aspekt szkolenia nakierowany jest na wspieranie wdrażania SMS.

11.6.4 Pierwszym krokiem we wdrażaniu SSP bezpośrednio dotyczącym wspierania wdrażania SMS jest stworzenie wymogów dotyczących SMS podmiotów lotniczych oraz wytycznych dotyczących wdrażania SMS. Wskazówki na temat tworzenia przepisów państwowych zawarte są w Dodatku 1 do rozdziału 10. Wskazówki te odwołują się do składników i elementów podstaw SMS wg ICAO omówionych w rozdziale 8. Niniejszy podręcznik oraz opracowane przez ICAO kursy SMS i SSP były źródłami użytymi przy tworzeniu wskazówek.

11.6.5 Drugim krokiem we wdrażaniu SSP bezpośrednio dotyczącym wspierania wdrażania SMS jest rewizja polityki zapewnienia przestrzegania przepisów przez władzę nadzorującą lotnictwo cywilne. Ten krok wymaga szczególnego podkreślenia.

11.6.6 Istotą zarówno SSP, jak i SMS jest uprzedzanie ryzyk związanych z bezpieczeństwem poprzez stworzenie zdolności do zarządzania bezpieczeństwem w ramach władz państwa i w sektorze lotniczym, zamiast oczekiwania na wypadki, incydenty lub przypadki nieprzestrzegania przepisów. Jednym z kluczowych elementów

zarządzania, jak pokazano w różnych częściach niniejszego podręcznika, jest pomiar, gdyż nie jest możliwym zarządzanie czymś, czego nie da się zmierzyć. Pomiar z kolei wymaga danych. Zatem zbieranie, analizowanie i wymiana danych związanych z bezpieczeństwem są w centrum interaktywnej natury SSP i SMS omówionej w punkcie 11.4.10.

11.6.7 Podczas normalnych czynności zarządzania bezpieczeństwem w ramach SSP i SMS, odpowiednio państwo i podmioty lotnicze wymieniają dane związane z bezpieczeństwem. Dane podmiotu lotniczego otrzymane przez państwo to dane indywidualne, z których część państwo przekształci w dane ogólne. Istotna ilość tych danych będzie oczywiście odnosić się do problemów zidentyfikowanych podczas normalnego funkcjonowania procesów SMS w podmiotach lotniczych. Jeżeli odpowiedzią władzy nadzorującej lotnictwo cywilne będzie zastosowanie środków administracyjnych, proces zarządzania bezpieczeństwem przez państwo stanie w miejscu. Dlatego też jest istotne, aby w ramach SSP, władza nadzorująca lotnictwo cywilne zrewidowała swą politykę zapewnienia przestrzegania przepisów w celu zapewnienia ciągłego napływu i wymiany danych z podmiotami lotniczymi działającymi w oparciu o SMS, danych umożliwiających proaktywne i przewidujące zarządzanie bezpieczeństwem. Proponuje się następujące wskazówki do uwzględnienia przy takiej rewizji:

a) należy pozwolić podmiotom lotniczym rozwiązywać niektóre problemy związane z bezpieczeństwem samodzielnie w ramach ich SMS;

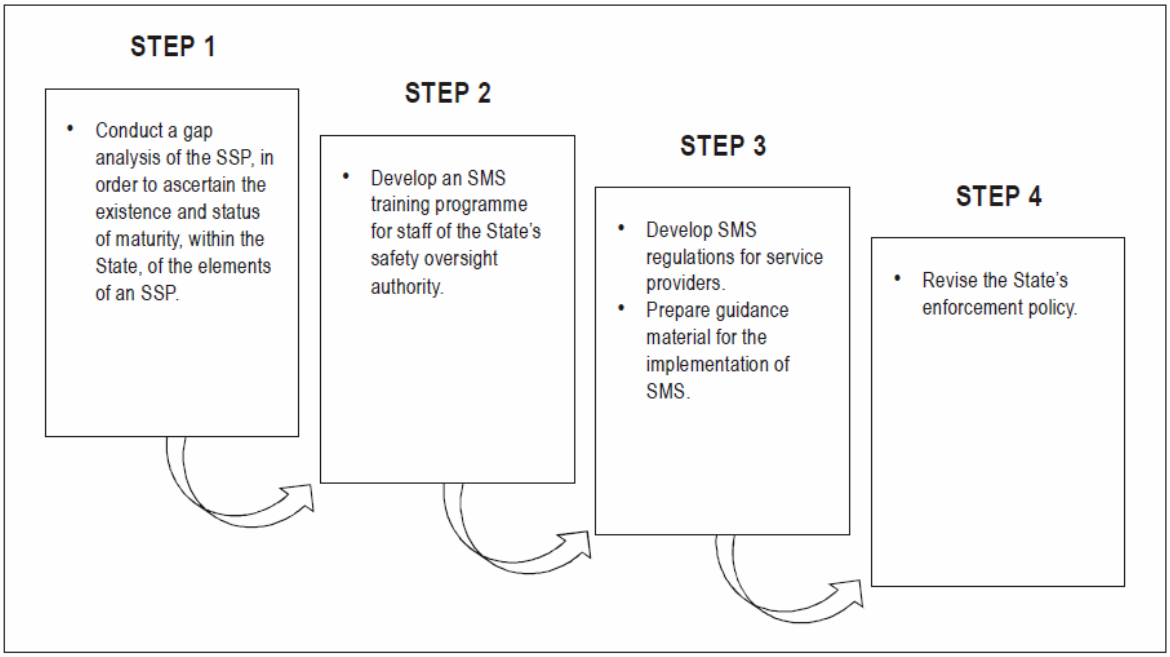
b) podmioty lotnicze powinny przedstawić państwu jasną definicję problemu związanego z bezpieczeństwem (*safety concern*), w tym odchyleń i/lub drobnych naruszeń oraz satysfakcjonujący dla Państwa plan ograniczania tych zjawisk;

c) plan ograniczania powinien zawierać harmonogramy, aby państwo mogło monitorować postęp;

d) w przypadkach poważnych zaniedbań, zachowań lekkomyślnych oraz zamierzonych przekroczeń należy postępować zgodnie z ustalonymi procedurami administracyjnymi.

Dodatek 4 do niniejszego rozdziału zawiera wytyczne dotyczące ustanowienia polityki zapewnienia przestrzegania przepisów przez państwo oraz odpowiednich procedur w środowisku SMS.

11.6.8 Podsumowanie roli SSP we wspieraniu wdrażania SMS ukazuje rysunek 11-2.




**Rysunek 11-2. Podsumowanie roli SSP we wspieraniu wdrażania SMS**

## Dodatek 1 do Rozdziału 11

# RAMY KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA (SSP)

*Uwaga.— W niniejszym Dodatku termin „podmiot lotniczy" odnosi się do każdej organizacji świadczącej usługi lotnicze. Pojęcie to obejmuje zatwierdzone organizacje szkoleniowe narażone na ryzyko w czasie świadczenia usług, użytkowników statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projektowanie i produkcję statków powietrznych, służby ruchu lotniczego i certyfikowane lotniska.*

Niniejszy Dodatek wprowadza podstawy dla wdrożenia i realizowania krajowego programu bezpieczeństwa (SSP) przez Państwo. Podstawy te zawierają następujące cztery składniki i jedenaście elementów:

1. Polityka i cele Państwa w zakresie bezpieczeństwa

   1.1 obowiązujące w Państwie przepisy dotyczące bezpieczeństwa;

   1.2 określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo;

   1.3 badanie wypadków i incydentów;

   1.4 polityka zapewniania przestrzegania przepisów.

2. Zarządzanie ryzykiem przez Państwo

   2.1 wymagania dotyczące SMS podmiotów lotniczych;

   2.2 uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.

3. Zapewnianie bezpieczeństwa przez Państwo

   3.1 nadzór nad bezpieczeństwem;

   3.2 zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa;

   3.3 ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach.

4. Promowanie bezpieczeństwa przez Państwo

   4.1 wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa;

   4.2 zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

Poniżej znajduje się krótki opis każdego z elementów.

## 1. POLITYKA I CELE PAŃSTWA W ZAKRESIE BEZPIECZEŃSTWA

### 1.1 Obowiązujące w Państwie przepisy dotyczące bezpieczeństwa

Państwo ustanawia ramowe i szczegółowe przepisy, zgodne ze standardami międzynarodowymi i krajowymi, określające zarządzanie bezpieczeństwem przez Państwo. Obejmuje to uczestnictwo instytucji Państwowych w konkretnych działaniach związanych z zarządzaniem bezpieczeństwem w Państwie oraz określenie ról, zakresów odpowiedzialności i powiązań pomiędzy tymi instytucjami. W celu zapewnienia aktualności i odpowiedniości, ogólne podstawy prawne oraz konkretne regulacje podlegają okresowemu przeglądowi.

### 1.2 Określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo

Państwo identyfikuje, definiuje i dokumentuje wymagania i zakresy odpowiedzialności związane z ustanowieniem i funkcjonowaniem SSP. Obejmuje to wytyczne dla planowania, organizowania, tworzenia, kontrolowania i ciągłego ulepszania SSP w sposób spełniający cele Państwa w dziedzinie bezpieczeństwa. Punkt ten zawiera również jasną deklarację w sprawie przeznaczenia zasobów koniecznych do wdrażania SSP.

### 1.3 Badanie wypadków i incydentów

Państwo ustanawia niezależny proces badania wypadków i incydentów, którego jedynym celem jest zapobieganie wypadkom i incydentom, a nie określanie winy bądź odpowiedzialności. Badania takie wspierają zarządzanie bezpieczeństwem w Państwie. W czasie funkcjonowania SSP Państwo utrzymuje niezależność instytucji badającej wypadki i incydenty od innych instytucji Państwa odpowiedzialnych za lotnictwo.

### 1.4 Polityka zapewniania przestrzegania przepisów

Państwo publikuje politykę zapewniania przestrzegania przepisów, w której określa warunki i okoliczności, w których podmiotom lotniczym zezwala się na prowadzenie wewnętrznego postępowania przy zdarzeniach związanych z niektórymi naruszeniami, w ramach SMS danego podmiotu i za aprobatą właściwej władzy Państwowej. Polityka ta określa również warunki i okoliczności, w których naruszenia podlegają określonej procedurze administracyjnej.

## 2. ZARZĄDZANIE RYZYKIEM PRZEZ PAŃSTWO

### 2.1 Wymagania dotyczące SMS podmiotów lotniczych

Państwo ustanawia zasady określające, jak podmioty lotnicze będą identyfikować zagrożenia i zarządzać ryzykiem. Obejmuje to wymagania, szczegółowe przepisy operacyjne i polityki wdrażania dotyczące SMS podmiotów lotniczych. Dokumenty te podlegają okresowej rewizji, aby były aktualne i odpowiednie dla podmiotów lotniczych.

### 2.2 Uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych

Państwo uzgadnia z poszczególnymi podmiotami lotniczymi warunki ich SMS. Uzgodnione warunki bezpieczeństwa SMS podmiotu lotniczego podlegają okresowej rewizji, aby były aktualne i odpowiednie dla podmiotu.

## 3. ZAPEWNIANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

### 3.1 Nadzór nad bezpieczeństwem

Państwo ustanawia mechanizmy zapewniające skuteczne monitorowanie ośmiu elementów krytycznych bezpieczeństwa. Państwo ustanawia również mechanizmy zapewniające, że identyfikacja zagrożeń i zarządzanie ryzykiem przez podmioty lotnicze są zgodne z ustalonymi zasadami (wymaganiami, szczegółowymi przepisami operacyjnymi i polityką wdrażania). Mechanizmy te obejmują inspekcje, audyty i ankiety, mające zapewnić, że zasady ustanowione przez Państwo są właściwie odzwierciedlone w SMS podmiotu lotniczego, i że stosowane są tak jak to przewidziano, a ustanowione zasady wywierają założony wpływ na ryzyko.

### 3.2 Zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa

Państwo ustanawia mechanizmy pozwalające na zbieranie i przechowywanie danych o zagrożeniach i ryzykach zarówno na poziomie indywidualnym, jak i w formie ogólnej, na poziomie krajowym. Państwo ustanawia również mechanizmy tworzenia informacji z zebranych danych i aktywnej wymiany informacji z podmiotami lotniczymi i/lub innymi Państwami.

### 3.3 Ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach

Państwo ustanawia procedury i priorytety inspekcji, audytów i ankiet w obszarach o największych problemach lub potrzebach związanych z bezpieczeństwem, zidentyfikowanych podczas analizy danych o zagrożeniach, ich konsekwencjach operacyjnych i ustalonych ryzykach.

## 4. PROMOWANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

### 4.1 Wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa

Państwo prowadzi szkolenia, działania uświadamiające i utrzymuje dwustronną wymianę informacji istotnych z punktu widzenia bezpieczeństwa, wspierającą budowę w instytucjach lotniczych Państwa kultury sprzyjającej skutecznemu i wydajnemu SSP.

### 4.2 Zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa

Państwo prowadzi działania edukacyjne i uświadamiające oraz utrzymuje dwustronną wymianę informacji istotnych z punktu widzenia bezpieczeństwa, wspierającą budowę w podmiotach lotniczych kultury sprzyjającej skutecznemu i wydajnemu SMS.

— — — — — — — — —

## Dodatek 2 do Rozdziału 11

# WYTYCZNE DOTYCZĄCE TWORZENIA DEKLARACJI PAŃSTWA W ZAKRESIE BEZPIECZEŃSTWA

Zarządzanie bezpieczeństwem lotnictwa cywilnego jest jednym z głównych obszarów odpowiedzialności [Państwa]. [Państwo] zobowiązuje się do tworzenia, wdrażania, utrzymywania oraz ciągłego ulepszania strategii i procesów w celu zapewnienia, że wszelka nadzorowana przez nie działalność lotnicza prowadzona jest przy zachowaniu najwyższego poziomu bezpieczeństwa, w zgodzie ze standardami krajowymi i międzynarodowymi.

Posiadacze certyfikatów lotniczych wydanych przez [Państwo] muszą udowodnić, że ich systemy zarządzania odzwierciedlają podejście oparte na SMS. Oczekiwanym rezultatem takiego podejścia jest lepsze zarządzanie bezpieczeństwem i działania zapewniające bezpieczeństwo, w tym zgłaszanie informacji związanych z bezpieczeństwem w sektorze lotnictwa cywilnego.

W [Państwie] wszystkie szczeble zarządzania odpowiedzialne są za utrzymanie najwyższego poziomu bezpieczeństwa, począwszy od Odpowiedzialnego Dyrektora (odpowiedniego dla danej organizacji).

[Państwo] zobowiązuje się do:

a) stworzenia ogólnych przepisów i konkretnych polityk operacyjnych wykorzystujących zasady zarządzania bezpieczeństwem, opartych na całościowej analizie systemu lotniczego Państwa;

b) konsultowania spraw związanych z rozwojem przepisów ze wszystkimi segmentami sektora lotniczego;

c) wspierania zarządzania bezpieczeństwem w Państwie poprzez skuteczny system zgłaszania i komunikowania;

d) efektywnego utrzymywania interakcji z podmiotami lotniczymi przy rozwiązywaniu problemów związanych z bezpieczeństwem;

e) zapewnienia, że [władzy nadzorującej bezpieczeństwo w Państwie] przekazano wystarczające zasoby, a jej personel posiada odpowiednie umiejętności i został przeszkolony do wykonywania swoich zadań, zarówno związanych z bezpieczeństwem, jak i pozostałych;

f) prowadzenia czynności nadzoru nad bezpieczeństwem zarówno zorientowanych na wyniki, jak i skupionych na kontroli przestrzegania przepisów, wspieranych analizami oraz alokacją zasobów wg kryteriów ryzyka dla bezpieczeństwa;

g) utrzymania zgodności z międzynarodowymi standardami i wymaganiami dotyczącymi bezpieczeństwa, a gdzie to możliwe – ustanawiania dalej idących rozwiązań;

h) promowania koncepcji i zasad zarządzania bezpieczeństwem oraz edukowania sektora lotniczego w tym zakresie;

i) nadzorowania wdrażania SMS w organizacjach lotniczych;

j) zapewnienia, że wszelka nadzorowana przez nie działalność utrzymuje najwyższy standard bezpieczeństwa;

k) ustanowienia środków ochrony systemów zbierania i przetwarzania informacji z zakresu bezpieczeństwa (SDCPS), aby zachęcić do przekazywania istotnych danych o zagrożeniach i utrzymania ciągłego przepływu informacji pomiędzy [Państwem] a podmiotami lotniczymi;

l) ustanowienia i monitorowania realnego wdrażania SSP wobec jasno określonych wskaźników i celów;

m) wydania polityki zapewnienia przestrzegania przepisów, która zapewni, że żadne informacje uzyskane z jakichkolwiek SDCPS ustanowionych w ramach SSP lub SMS nie staną się podstawą do czynności dyscyplinarnych, poza przypadkami poważnych zaniedbań lub celowego łamania przepisów.

Polityka ta musi być zrozumiana, wdrażana i przestrzegana przez wszystkich pracowników zaangażowanych w działania [władzy sprawującej nadzór nad bezpieczeństwem].

(Podpis) _____
Dyrektor Odpowiedzialny

— — — — — — — — —

## Dodatek 3 do Rozdziału 11

# WYTYCZNE W SPRAWIE ANALIZY LUK KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA (SSP)

*Uwaga.— W niniejszym Dodatku termin „podmiot lotniczy" odnosi się do każdej organizacji świadczącej usługi lotnicze. Pojęcie to obejmuje zatwierdzone organizacje szkoleniowe narażone na ryzyko w czasie świadczenia usług, użytkowników statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projektowanie i produkcję statków powietrznych, służby ruchu lotniczego, i certyfikowane lotniska.*

### 1. ANALIZA LUK

1.1 Aby wdrożyć SSP Państwo musi przeprowadzić analizę swego systemu bezpieczeństwa, aby ustalić, które składniki i elementy SSP już istnieją, a które należy dodać bądź przekształcić w celu spełnienia wymagań. Analiza taka jest znana pod nazwą analizy luk i polega na porównywaniu wymagań dotyczących SSP z istniejącymi zasobami Państwa.

1.2 Analiza luk dostarcza, w formie listy kontrolnej, informacji pomagających w ocenie istniejących składników i elementów podstaw SSP wg ICAO, i w określeniu, które składniki i elementy należy rozwinąć. Gdy analiza luk zostanie ukończona i udokumentowana, stanie się jedną z podstaw planu wdrażania SSP.

### 2. PODSTAWY SSP WG ICAO

Podstawy SSP wg ICAO zawierają następujące cztery składniki i jedenaście elementów:

1. Polityka i cele Państwa w zakresie bezpieczeństwa
   - 1.1 obowiązujące w Państwie przepisy dotyczące bezpieczeństwa;
   - 1.2 określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo;
   - 1.3 badanie wypadków i incydentów;
   - 1.4 polityka zapewniania przestrzegania przepisów.
2. Zarządzanie ryzykiem przez Państwo
   - 2.1 wymagania dotyczące SMS podmiotów lotniczych;
   - 2.2 uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.
3. Zapewnianie bezpieczeństwa przez Państwo
   - 3.1 nadzór nad bezpieczeństwem;
   - 3.2 zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa;
   - 3.3 ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach.

4. Promowanie bezpieczeństwa przez Państwo

4.1 wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa;

4.2 zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

### 3. ANALIZA LUK KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA (SSP)

Poniższa lista kontrolna analizy luk może zostać wykorzystana jako formularz do przeprowadzenia analizy luk. Na każde pytanie można odpowiedzieć „Tak" lub „Nie". Odpowiedź „Tak" oznacza, że Państwo włączyło już dany składnik lub element podstaw SSP wg ICAO do swego systemu bezpieczeństwa. Odpowiedź „Nie" oznacza, że istnieje luka pomiędzy składnikiem/elementem podstaw SSP wg ICAO a systemem bezpieczeństwa w Państwie.

| Odniesienie w dokumencie ICAO (Doc 9859) | Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi | Odpowiedź | Status implementacji |
|---|---|---|---|
| **Składnik 1 - POLITYKA I CELE PAŃSTWA W ZAKRESIE BEZPIECZEŃSTWA** | | | |
| **Element 1.1 - Obowiązujące w Państwie przepisy dotyczące bezpieczeństwa** | | | |
| Rozdział 11 | Czy [Państwo] ustanowiło krajowe przepisy prawne i szczegółowe regulacje w dziedzinie bezpieczeństwa? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] określiło konkretne działania związane z zarządzaniem bezpieczeństwem w [Państwie], w których musi uczestniczyć każda organizacja lotnicza? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] ustanowiło wymagania oraz zakresy odpowiedzialności związane z zarządzaniem bezpieczeństwem przez jego władze lotnicze? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ramy prawne i szczegółowe regulacje podlegają okresowemu przeglądowi, aby pozostały aktualne i odpowiednie dla Państwa? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ramy prawne i szczegółowe regulacje podlegają okresowemu przeglądowi, aby pozostały w zgodności ze standardami międzynarodowymi? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] zatwierdziło politykę bezpieczeństwa? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy polityka bezpieczeństwa [Państwa] została podpisana przez Dyrektora Odpowiedzialnego za SSP lub przez wysoką władzę [Państwa]? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy polityka bezpieczeństwa [Państwa] podlega okresowej rewizji? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy polityka bezpieczeństwa [Państwa] jest komunikowana z odpowiednim naciskiem wszystkim pracownikom organizacji lotniczych [Państwa] z intencją, aby brali ją pod uwagę podczas wykonywania indywidualnych obowiązków związanych z bezpieczeństwem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] wydało dokumentację opisującą SSP, w tym związki pomiędzy poszczególnymi elementami? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy Państwo posiada system gromadzenia danych umożliwiający generowanie i archiwizowanie wszelkich danych niezbędnych do udokumentowania i wspierania działań w ramach SSP? | ☐ Tak<br>☐ Nie | |

| | | | |
|---|---|---|---|
| Rozdział 11 | Czy system gromadzenia danych zawiera procesy kontrolne zapewniające odpowiednią identyfikację, czytelność, przechowywanie, ochronę, archiwizację, odzyskiwanie, czas przechowywania i dysponowanie danymi? | ☐ Tak<br>☐ Nie | |
| **Element 1.2 - Określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo** | | | |
| Rozdział 11 | Czy [Państwo] określiło i zdefiniowało urzędowe wymagania i zakresy odpowiedzialności odnoszące się do ustanowienia i funkcjonowania SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy wymagania te zawierają dyrektywy i działania w celu planowania, organizowania, rozwijania, kontrolowania i ciągłego ulepszania SSP w sposób spełniający cele [Państwa] w dziedzinie bezpieczeństwa? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy wymagania te zawierają jasną deklarację co do zapewnienia zasobów koniecznych do wdrożenia i funkcjonowania SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] określiło i powołało Odpowiedzialnego Dyrektora jako osobę posiadającą odpowiednie kwalifikacje i bezpośrednią odpowiedzialność za wdrażanie, funkcjonowanie i nadzór nad SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy Dyrektor Odpowiedzialny za SSP w [Państwie] wypełnia wymagane funkcje i zadania? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy Dyrektor Odpowiedzialny za SSP w [Państwie] odpowiednio koordynuje działania różnych struktur lotniczych Państwa w ramach SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy Dyrektor Odpowiedzialny za SSP w [Państwie] posiada zasoby niezbędne do prawidłowego wdrażania SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy Dyrektor Odpowiedzialny za SSP w [Państwie] sprawdza, czy wszyscy pracownicy struktur lotniczych [Państwa] rozumieją swoje uprawnienia i zakresy odpowiedzialności w ramach SSP i wszystkich procesów, decyzji i działań związanych z zarządzaniem bezpieczeństwem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy zakresy odpowiedzialności są zdefiniowane i udokumentowane na wszystkich szczeblach? | ☐ Tak<br>☐ Nie | |
| **Element 1.3 – Badanie wypadków i incydentów** | | | |
| Rozdział 11 | Czy [Państwo] w ramach zarządzania bezpieczeństwem ustanowiło niezależny proces badania wypadków i incydentów, którego jedynym celem jest zapobieganie wypadkom i incydentom, a nie wskazanie winnych lub odpowiedzialnych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] utrzymuje niezależność organizacji badającej wypadki i incydenty od innych Państwowych organizacji lotniczych? | ☐ Tak<br>☐ Nie | |
| **Element 1.4 – Polityka zapewnienia przestrzegania przepisów** | | | |
| Rozdział 11 | Czy [Państwo] ogłosiło politykę zapewnienia przestrzegania przepisów? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy polityka zapewnienia przestrzegania przepisów określa warunki i okoliczności, w których podmiotom lotniczym zezwala się na wewnętrzne procedowanie w sprawach zdarzeń związanych z przekroczeniami warunków bezpieczeństwa, w kontekście systemu zarządzania bezpieczeństwem danego podmiotu i za aprobatą właściwej władzy Państwowej? | ☐ Tak<br>☐ Nie | |

| | | | |
|---|---|---|---|
| Rozdział 11 | Czy polityka zapewnienia przestrzegania przepisów określa warunki i okoliczności, w których procedowanie w sprawach zdarzeń związanych z przekroczeniami warunków bezpieczeństwa podlega ustalonym procedurom administracyjnym? | ☐ Tak<br>☐ Nie | |
| **Składnik 2 – ZARZĄDZANIE RYZYKIEM PRZEZ PAŃSTWO** | | | |
| **Element 2.1 – Wymagania dotyczące SMS podmiotów lotniczych** | | | |
| Rozdział 11 | Czy [Państwo] ustanowiło reguły określające, jak podmioty lotnicze identyfikują zagrożenia i zarządzają ryzykiem związanym z bezpieczeństwem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy reguły te zawierają wymagania, konkretne przepisy operacyjne i polityki wdrażania dotyczące SMS podmiotów lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy wymagania, konkretne przepisy operacyjne i polityki wdrażania oparte są na zidentyfikowanych zagrożeniach i analizie ryzyka wynikającego z konsekwencji zagrożeń? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy wymagania, konkretne przepisy operacyjne i polityki wdrażania podlegają okresowemu przeglądowi tak, aby pozostały aktualne i odpowiednie dla podmiotów lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy w [Państwie] istnieje strukturyzowany proces oceny zarządzania przez podmioty lotnicze ryzykiem związanym ze zidentyfikowanymi zagrożeniami, wyrażony w kategoriach prawdopodobieństwa i dotkliwości skutków wystąpienia? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] posiada politykę zapewniającą efektywne zgłaszanie niedociągnięć w zakresie bezpieczeństwa, zagrożeń i zdarzeń? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy polityka [Państwa] w zakresie zgłaszania niedociągnięć, zagrożeń lub zdarzeń zawiera warunki przyznawania ochrony przed krokami dyscyplinarnymi i/lub administracyjnymi? | ☐ Tak<br>☐ Nie | |
| **Element 2.2 - Uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych** | | | |
| Rozdział 11 | Czy [Państwo] uzgodniło indywidualnie z podmiotami lotniczymi parametry ich SMS? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy uzgodnione parametry bezpieczeństwa są współmierne ze stopniem złożoności kontekstu operacyjnego danego podmiotu lotniczego? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy uzgodnione parametry bezpieczeństwa uwzględniają możliwości danego podmiotu w zakresie zarządzania ryzykiem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy uzgodnione parametry bezpieczeństwa wyrażone są poprzez liczne (a nie pojedyncze) wskaźniki i cele bezpieczeństwa oraz plany działania? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy uzgodnione parametry bezpieczeństwa podlegają okresowej rewizji, aby pozostały aktualne i odpowiednie dla podmiotu lotniczego? | ☐ Tak<br>☐ Nie | |

| | | | |
|---|---|---|---|
| **Składnik 3 – ZAPEWNIANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO** | | | |
| **Element 3.1 – Nadzór nad bezpieczeństwem** | | | |
| Rozdział 11 | Czy [Państwo] ustanowiło mechanizmy zapewniające skuteczną funkcję nadzoru nad bezpieczeństwem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] ustanowiło mechanizmy zapewniające, że identyfikacja zagrożeń i zarządzanie ryzykiem w obszarze bezpieczeństwa przez podmioty lotnicze prowadzone są zgodnie z wymaganiami? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ustanowione mechanizmy obejmują inspekcje, audyty i ankiety po to, by regulacje dotyczące ryzyka były prawidłowo włączone do SMS podmiotów lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ustanowione mechanizmy zapewniają, że wymagania są wdrażane tak jak zaplanowano? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ustanowione mechanizmy zapewniają, że wymagania dotyczące kontroli ryzyka odnoszą założony wpływ na ryzyka związane z bezpieczeństwem? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy przeprowadza się regularne, okresowe rewizje ALoS [Państwa]? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy podczas rewizji rozpatruje się zmiany, które mogłyby wpłynąć na SSP [Państwa] i jego ALoS, zalecenia co do ulepszenia programu oraz wymiany najlepszych praktyk? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy przeprowadza się regularne, okresowe rewizje w celu ustalenia czy SSP i ALoS [Państwa] pozostają odpowiednie dla rozmiarów i złożoności operacji lotniczych w Państwie? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy istnieje proces ewaluacji zmian związanych z SSP? | ☐ Tak<br>☐ Nie | |
| **Element 3.2 – Zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa** | | | |
| Rozdział 11 | Czy [Państwo] ustanowiło mechanizmy zapewniające zbieranie i przechowywanie danych na temat zagrożeń i ryzyka zarówno na szczeblu Państwa, jak i indywidualnych podmiotów lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] ustanowiło mechanizmy pozyskiwania informacji z przechowywanych danych oraz promowania wymiany danych dotyczących bezpieczeństwa z podmiotami lotniczymi i /lub innymi Państwami? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy [Państwo] określiło akceptowalny poziom bezpieczeństwa (ALoS) związany z SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ALoS [Państwa] łączy w sobie elementy pomiaru bezpieczeństwa i pomiaru parametrów bezpieczeństwa? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy ALoS [Państwa] jest współmierny do stopnia złożoności działalności lotniczej w [Państwie]? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy funkcjonuje w [Państwie] formalny proces tworzenia i utrzymywania zestawu parametrów do pomiaru rzeczywistego wdrażania SSP? | ☐ Tak<br>☐ Nie | |
| **Element 3.3 – Ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach** | | | |
| Rozdział 11 | Czy [Państwo] ustanowiło procedury ukierunkowujące inspekcje, audyty i badania na obszary wymagające szczególnej uwagi i o największych potrzebach? | ☐ Tak<br>☐ Nie | |

| | | | |
|---|---|---|---|
| Rozdział 11 | Czy ukierunkowanie inspekcji i audytów jest wynikiem analizy danych o zagrożeniach i ich konsekwencjach operacyjnych oraz ocenionym ryzyku dla bezpieczeństwa? | ☐ Tak<br>☐ Nie | |
| **Składnik 4 – PROMOWANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO** | | | |
| **Element 4.1 – Wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa** | | | |
| Rozdział 11 | Czy [Państwo] zapewnia wewnętrzne szkolenia, akcje uświadamiające i dwustronne komunikowanie informacji mających znaczenie dla bezpieczeństwa w państwowych strukturach lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy istnieją w [Państwie] procesy komunikacyjne zapewniające na czas strukturom lotniczym Państwa dostępność informacji na temat funkcji i wytworów SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy istnieje proces upowszechniania informacji dotyczących bezpieczeństwa w strukturach lotniczych [Państwa] i mechanizmy monitorowania efektywności tego procesu? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy procesy komunikacyjne (pisma, spotkania, komunikacja elektroniczna) są współmierne do rozmiaru i obszaru działania struktur lotniczych [Państwa]? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy informacje dotyczące bezpieczeństwa i na temat funkcji i wytworów SSP są przechowywane na odpowiednim nośniku? | ☐ Tak<br>☐ Nie | |
| **Element 4.2 – Zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa** | | | |
| Rozdział 11 | Czy [Państwo] zapewnia zewnętrzne szkolenia, akcje uświadamiające i dwustronne komunikowanie informacji mających znaczenie dla bezpieczeństwa w państwowych strukturach lotniczych? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy wdrożone zostały w [Państwie] procesy komunikacyjne umożliwiające promowanie SSP w kraju i za granicą? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy istnieje formalny proces zewnętrznego upowszechniania informacji związanych z bezpieczeństwem wśród podmiotów lotniczych w [Państwie] i mechanizm monitorowania efektywności tego procesu? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy istnieją w [Państwie] procesy komunikacyjne zapewniające na czas podmiotom lotniczym dostępność informacji na temat funkcji i wytworów SSP? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy procesy komunikacyjne (pisma, spotkania, komunikacja elektroniczna) są współmierne do rozmiaru i obszaru działania podmiotów lotniczych w [Państwie]? | ☐ Tak<br>☐ Nie | |
| Rozdział 11 | Czy informacje dotyczące bezpieczeństwa i na temat funkcji i wytworów SSP są przechowywane na odpowiednim nośniku? | ☐ Tak<br>☐ Nie | |

— — — — — — — — —

## Dodatek 4 do Rozdziału 11

# WYTYCZNE NA TEMAT TWORZENIA POLITYKI ZAPEWNIENIA PRZESTRZEGANIA PRZEPISÓW I ZWIĄZANYCH Z NIĄ PROCEDUR W ŚRODOWISKU SMS

## POLITYKA ZAPEWNIENIA PRZESTRZEGANIA PRZEPISÓW

### 1. WSTĘP

Niniejsza polityka wydana została na podstawie upoważnienia [zawartego we właściwych przepisach państwowych dotyczących lotnictwa cywilnego, dekretu(ów) o żegludze powietrznej lub standardów regulacyjnych].

### 2. ZASADY

2.1 Niniejsza polityka jest efektem całościowego przeglądu regulacji i możliwości [Państwowego organu nadzoru lotniczego] w zakresie oceny działań podmiotów lotniczych w dziedzinie bezpieczeństwa.

2.2 Wdrożenie systemów zarządzania bezpieczeństwem (SMS) wymaga, aby [Państwowy organ nadzoru lotniczego] wypracował elastyczne podejście w zapewnianiu przestrzegania przepisów, dostosowane do nowych warunków, jednocześnie wykonując funkcję nadzoru nad przestrzeganiem przepisów w sposób sprawiedliwy, praktyczny i spójny. Elastyczne podejście do nadzoru nad przestrzeganiem przepisów w środowisku SMS powinno opierać się na dwóch ogólnych zasadach.

2.3 Pierwszą ogólną zasadą jest stworzenie procedur zapewnienia przestrzegania przepisów, które pozwolą podmiotom lotniczym na wewnętrzne postępowanie w przypadku niektórych zdarzeń obejmujących przekroczenia warunków bezpieczeństwa, w kontekście SMS danego podmiotu i za aprobatą władz. Świadome łamanie [ustawy o prawie lotniczym] i [przepisów wykonawczych] będzie przedmiotem dochodzenia i może podlegać zwyczajnym sankcjom administracyjnym.

2.4 Druga zasada ogólna stanowi, że informacje uzyskane z systemów zbierania i przetwarzania danych dotyczących bezpieczeństwa ustanowionych w ramach SMS nie mogą być podstawą do działań o charakterze administracyjnym.

### 3. ZAKRES

3.1 Zasady, na których opiera się niniejsza polityka oraz związane z nią procedury mają zastosowanie do podmiotów lotniczych działających zgodnie z Załącznikiem 1 – *Licencjonowanie personelu*; Załącznikiem 6 – *Eksploatacja statków powietrznych*, Część I - *Międzynarodowy, zarobkowy transport lotniczy – statek powietrzny* i Część III - *Operacje międzynarodowe – śmigłowce*; Załącznikiem 8 – *Zdatność do lotu statków powietrznych*; Załącznikiem 11 – *Służby ruchu lotniczego* i Załącznikiem 14, Tom I - *Projektowanie i eksploatacja lotnisk.*

3.2 W kontekście niniejszych wytycznych pojęcie „podmiot lotniczy” odnosi się do każdej organizacji dostarczającej usługi lotnicze. Pojęcie to obejmuje zatwierdzone organizacje szkoleniowe wystawione na zagrożenia podczas świadczenia usług, użytkowników statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projektowanie i/lub produkcję statków powietrznych, dostawców usług ruchu lotniczego i certyfikowane lotniska.

## 4. POSTANOWIENIA OGÓLNE

4.1 [Podmiot lotniczy] ustanowi i zapewni funkcjonowanie SMS współmiernego do jego rozmiaru oraz charakteru i stopnia złożoności operacji, do których upoważnia go posiadany certyfikat, a także współmiernego do zagrożeń i ryzyk związanych z tymi operacjami.

4.2 W celu stworzenia polityki zapewnienia przestrzegania przepisów wspierającej wdrożenie SMS, inspektorzy [Państwowego organu nadzoru lotniczego] będą prowadzić otwarty dialog z podmiotami lotniczymi.

4.3 Kiedy podmiot lotniczy działający zgodnie z SMS nieumyślnie przekracza przepisy [ustawy o lotnictwie cywilnym, przepisy lotnictwa cywilnego], użyte będą specjalne procedury badania. Procedury te pozwolą inspektorowi [Państwowego nadzoru lotniczego] odpowiedzialnemu za nadzór nad podmiotem rozpocząć z nim dialog. Celem dialogu będzie uzgodnienie zaproponowanych działań naprawczych i planu działania, który będzie odpowiadał charakterowi niedociągnięć, które doprowadziły do naruszeń i zapewni podmiotowi lotniczemu rozsądny czas na wdrożenie działań naprawczych. Podejście to ma na celu promowanie i wspieranie efektywnego zgłaszania zdarzeń, dzięki któremu pracownicy podmiotów lotniczych mogą zgłaszać niedociągnięcia i zagrożenia bez obawy przed ukaraniem. Podmiot lotniczy może więc, bez obawy przed działaniami administracyjnymi, przeanalizować zdarzenie i czynniki organizacyjne lub indywidualne, które mogły do niego doprowadzić, w celu zastosowania środków naprawczych, które pomogą zapobiec ponownemu wystąpieniu zdarzeń.

## 5. ŚRODKI NAPRAWCZE

[Państwowy organ nadzoru lotniczego ] za pośrednictwem inspektora odpowiedzialnego za nadzór nad danym podmiotem lotniczym oceni środki naprawcze zaproponowane przez podmiot oraz aktualnie istniejące systemy, w celu ustalenia zdarzenia leżącego u podstaw złamania przepisów. Jeżeli środki naprawcze zostaną uznane za właściwe i rokujące zapobieżenie ponownemu wystąpieniu zdarzenia oraz sprzyjające przestrzeganiu przepisów w przyszłości, postępowanie w związku ze zdarzeniem będzie zakończone bez żadnych sankcji. W przypadku, gdy zaproponowane środki naprawcze lub istniejące systemy okażą się niewystarczające, [Państwowy organ nadzoru lotniczego] będzie dalej kontaktował się z podmiotem lotniczym, aby znaleźć zadowalające rozwiązanie pozwalające uniknąć zastosowania sankcji. Jednakże, jeżeli podmiot lotniczy odmówi podjęcia działań w związku ze zdarzeniem i przedstawienia skutecznych środków naprawczych [Państwowy organ nadzoru lotniczego] rozważy podjęcie sankcji lub innych działań administracyjnych.

## 6. PROCEDURY ZAPEWNIANIA PRZESTRZEGANIA PRZEPISÓW

Łamanie przepisów lotniczych może mieć wiele różnorodnych powodów, od autentycznego niezrozumienia przepisów, do lekceważenia bezpieczeństwa w lotnictwie. [Państwowy organ nadzoru lotniczego] posiada wiele procedur zapewniania przestrzegania przepisów, odpowiadających wymaganiom w sprawach bezpieczeństwa określonym w [odpowiednim akcie Państwowym] dla różnych sytuacji. Procedury te mogą prowadzić do różnorodnych działań:

a) doradztwo;

b) szkolenia naprawcze;

c) zmiana, zawieszenie lub cofnięcie uprawnień.

## 7. BEZSTRONNOŚĆ DZIAŁAŃ

Na decyzje mające na celu zapewnienie przestrzegania przepisów nie może mieć wpływu:

a) konflikt o charakterze osobistym;

b) względy takie jak płeć, rasa, religia, poglądy lub powiązania polityczne;

c) wpływy osobiste, polityczne lub finansowe uczestników postępowania.

### 8. PROPORCJONALNOŚĆ ŚRODKÓW

Decyzje mające na celu zapewnienie przestrzegania przepisów muszą być proporcjonalne do stwierdzonych naruszeń i związanego z nimi ryzyka, w oparciu o dwie zasady:

a) [Państwowy organ nadzoru lotniczego] podejmie działania przeciwko tym, którzy konsekwentnie i celowo prowadzą działalność niezgodną z przepisami obowiązującymi w lotnictwie cywilnym;

b) [Państwowy organ nadzoru lotniczego] będzie starał się edukować i wspierać szkolenie lub opiekę mentorską nad tymi, którzy wykazują wolę rozwiązania problemów związanych z bezpieczeństwem.

### 9. ZASADY SPRAWIEDLIWOŚCI I ODPOWIEDZIALNOŚCI

Decyzje mające na celu zapewnienie przestrzegania przepisów powinny:

a) być sprawiedliwymi i zgodnymi z właściwym procesem postępowania;

b) być przejrzystymi dla zainteresowanych;

c) brać pod uwagę okoliczności sprawy oraz postawę/czyny podmiotu lotniczego;

d) być spójnymi z działaniami/decyzjami podjętymi w podobnych okolicznościach;

e) podlegać odpowiedniej kontroli wewnętrznej i zewnętrznej.

### 10. WYJĄTKI

10.1 Niniejsza polityka nie ma zastosowania w sytuacjach, gdy istnieją dowody umyślnego działania w celu zatajenia złamania przepisów.

10.2 Niniejsza polityka nie ma zastosowania w sytuacjach, gdy środki identyfikacji zagrożeń i zarządzania ryzykiem podmiotu lotniczego nie budzą zaufania.

10.3 Niniejsza polityka nie ma zastosowania w sytuacji powtarzających się naruszeń. Powtarzające się naruszenia to sytuacja, gdy podmiot lotniczy w przeszłości [wskazać okres] dopuścił się takich samych lub podobnych naruszeń.

10.4 W takich okolicznościach będą zastosowane kary określone w tabeli (lub właściwym taryfikatorze) dołączonej do ustanowionych procedur zapewnienia przestrzegania przepisów.

(Podpis) _____
Dyrektor Odpowiedzialny za SSP

— — — — — — — — —

# Procedury zapewnienia przestrzegania przepisów w środowisku SMS

## 1. POSTANOWIENIA OGÓLNE

W ramach krajowego programu bezpieczeństwa [Państwa] (SSP) [Państwowy organ nadzoru lotniczego] odpowiada za nadzór nad posiadaczami certyfikatów, działającymi w środowisku SMS. Procedury zapewniania przestrzegania przepisów dostarczają wskazówek odpowiedzialnym za nadzór nad podmiotami lotniczymi działającymi w środowisku SMS poprzez doradzanie właściwej drogi postępowania w przypadku czynów lub zaniechań, aby skutecznie zapewnić przestrzeganie przepisów. Procedury te odgrywają rolę pomocniczą w programie, a ostateczna decyzja dotycząca działań zapewniających przestrzeganie przepisów należy do dyrektora odpowiedzialnego.

## 2. ZAKRES ZASTOSOWANIA

2.1 Procedury mają zastosowanie w przypadkach naruszeń popełnianych przez osoby lub podmioty lotnicze prowadzące działalność w kontekście SMS.

2.2 Procedury wchodzą w życie z [dniem]. Zastępują i odwołują poprzednie procedury określone we [właściwych przepisach lotniczych].

2.3 Jeżeli podmiot lotniczy okazał chęć prowadzenia działań zgodnie z SMS, procedury zapewniania przestrzegania przepisów zgodne z SMS mogą być zastosowane wobec naruszeń dokonanych przez ten podmiot, nawet jeśli nie posiada on zaakceptowanego SMS, ale wdrożył on niektóre kluczowe składniki SMS i jest w trakcie wdrażania całości SMS.

2.4 [Państwowy organ nadzoru lotniczego] nie zastosuje procedur zapewnienia przestrzegania przepisów w środowisku SMS do podmiotów lotniczych, które bezpodstawnie twierdzą, że opracowują SMS. Procedury te będą zaś zastosowane do podmiotów, które z należytą starannością zaangażowały się w opracowanie SMS, który spełniłby wymagania określone w przepisach dotyczących SMS i postępowały zgodnie z „podejściem etapowym" podobnym do opisanego w materiale doradczym [sygnatura] opublikowanym przez [Państwowy organ nadzoru lotniczego].

2.5 Jeżeli podmiot lotniczy nie wskaże, że działa w środowisku SMS, działania mające na celu zapewnienie przestrzegania przepisów będą miały zastosowanie bez korzyści wynikających z procedur opisanych w paragrafie 3.

## 3. PROCEDURY

3.1 W celu ustalenia, czy dochodzenie ma być prowadzone przy użyciu procedur zapewniania przestrzegania przepisów w środowisku SMS, koniecznym jest ustalenie statusu wdrożenia SMS przez dany podmiot lotniczy. Ustalenia takiego dokonuje się początkowo poprzez komunikację pomiędzy prowadzącymi dochodzenie a głównym inspektorem odpowiedzialnym za certyfikację i nadzór nad danym podmiotem.

3.2 Główny inspektor ustali, czy dany podmiot spełnia wyżej wymienione kryteria zastosowania procedur zapewniania przestrzegania przepisów w środowisku SMS. Aby ułatwić ocenę, [Państwowy organ nadzoru lotniczego] może sporządzić listę podmiotów, które rozpoczęły opracowywanie i wdrażanie SMS. Udostępnienie takiej listy prowadzącym dochodzenie pomoże im w podjęciu decyzji czy użyć tych procedur.

3.3 Przy „podejściu etapowym” do wdrażania SMS podmiotu lotniczego [Państwowy organ nadzoru lotniczego] zastosuje procedury zapewnienia przestrzegania przepisów wobec podmiotów lotniczych, które nie w pełni wdrożyły SMS, pod warunkiem spełnienia pewnych kryteriów.

3.4 [Państwowy organ nadzoru lotniczego] będzie wymagać, jako minimum konieczne do zastosowania procedur zapewniania przestrzegania przepisów w środowisku SMS, spełnienia trzech następujących warunków:

a) podmiot lotniczy posiada efektywny wewnętrzny program zgłaszania zagrożeń, wspierany przez wyższe kierownictwo;

b) podmiot lotniczy posiada proaktywny proces analizowania zdarzeń współmierny do jego rozmiaru i stopnia złożoności operacji oraz odpowiedniego do ustalania czynników przyczynowych i stosowania środków naprawczych;

c) informacje uzyskane w wyniku procesu opisanego w paragrafie 3 podlegające odpowiedniej ochronie (aby nie narażać SDCPS) są przekazywane na żądanie głównemu inspektorowi odpowiedzialnemu za dany podmiot.

**Wstępny raport o naruszeniu**

3.5 Inspektorzy prowadzący dochodzenie muszą dokonać wstępnej analizy we wszelkich przypadkach, gdy stwierdzono złamanie przepisów lub otrzymano informację o możliwym złamaniu przepisów.

**Analiza wstępna**

3.6 W oparciu o otrzymane informacje należy wziąć pod uwagę następujące kwestie:

a) Czy są uzasadnione podstawy, aby sądzić, że osoba lub organizacja prowadząca działalność w ramach SMS mogła popełnić naruszenie?

b) Czy charakter wydarzenia jest wystarczająco poważny, żeby uzasadniać podjęcie akcji mającej na celu zapewnienie przestrzegania przepisów?

c) Czy istnieją jakiekolwiek nietrwałe dowody, które powinny być zabezpieczone dla celów dochodzenia?

**Wsparcie**

3.7 Jeżeli na powyższe trzy pytania udzielono odpowiedzi pozytywnej, powinno się powiadomić głównego inspektora. Informacja powinna wskazywać zdarzenie i naruszenie przepisów.

3.8 Na żądanie Dyrektora Odpowiedzialnego prowadzący dochodzenie zapewnią odpowiednie wsparcie w formie sugerowania właściwych działań. Wsparcie dla Dyrektora Odpowiedzialnego obejmie również zbieranie i zabezpieczanie nietrwałych dowodów.

**Rozpoczęcie postępowania**

3.9 Postępowanie mające na celu zapewnienie przestrzegania przepisów może być rozpoczęte jedynie na wniosek głównego inspektora, a nie prowadzących dochodzenie.

**Immunitet**

3.10 Żadne informacje uzyskane z SDCPS nie będą używane jako podstawa do działań mających na celu zapewnienie przestrzegania przepisów.

*Uwaga.— Polityka zapewniania przestrzegania przepisów w środowisku SMS i związane z nią procedury może być również zastosowana do zagranicznych operatorów działających zgodnie z przepisami dotyczącymi SMS, spełniającymi wymagania i wytyczne Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO), spełniających kryteria określone w paragrafie 3.*

— — — — — — — — —

## Dodatek 5 do Rozdziału 11

# WYTYCZNE W SPRAWIE TWORZENIA PLANU WDRAŻANIA SSP

### 1. WSTĘP

1.1 Niniejszy Dodatek zawiera wytyczne mające pomóc Państwom w tworzeniu planu wdrażania SSP. Plan wdrażania SSP opisuje, jak Państwo wcieli w życie, we właściwej kolejności i zgodnie z zasadami, procesy, procedury i środki umożliwiające mu wykonywanie obowiązków związanych z zarządzaniem bezpieczeństwem w lotnictwie cywilnym.

1.2 Wdrożenie SSP musi być przeprowadzone w sposób odpowiedni dla rozmiaru i stopnia złożoności systemu lotniczego Państwa i może wymagać koordynacji pomiędzy wieloma instytucjami odpowiedzialnymi za poszczególne elementy funkcji Państwa w obszarze lotnictwa cywilnego. Niniejsze wytyczne mają być punktem odniesienia i mogą być modyfikowane w zależności od potrzeb Państw.

1.3 Tworzenie planu wdrażania SSP pozwoli Państwom:

a) sformułować ogólną strategię zarządzania bezpieczeństwem w Państwie;

b) skoordynować procesy wykonywane przez różne instytucje lotnicze Państwa w ramach SSP;

c) ustanowić reguły określające sposób funkcjonowania systemów zarządzania bezpieczeństwem (SMS) podmiotów lotniczych;

d) zapewnić, że funkcjonowanie SMS podmiotów lotniczych jest zgodne z ustanowionymi regułami;

e) wzmocnić interakcje pomiędzy SSP a funkcjonowaniem SMS podmiotów lotniczych.

1.4 Tam, gdzie Państwo odpowiada za świadczenie pewnych usług (np. lotniskowych, służb żeglugi powietrznej) jednostka świadcząca te usługi powinna opracować i wdrożyć SMS (patrz plan wdrażania SMS w Dodatku 2 do Rozdziału 10).

*Uwaga.— W niniejszym Dodatku termin „podmiot lotniczy" odnosi się do każdej organizacji świadczącej usługi lotnicze. Pojęcie to obejmuje zatwierdzone organizacje szkoleniowe narażone na ryzyko w czasie świadczenia usług, użytkowników statków powietrznych, zatwierdzone organizacje obsługowe, organizacje odpowiedzialne za projektowanie i produkcję statków powietrznych, służby ruchu lotniczego i certyfikowane lotniska.*

### 2. ANALIZA LUK SSP

2.1 W celu stworzenia planu wdrażania SSP, należy przeprowadzić analizę luk w istniejących w Państwie strukturach i procesach pod kątem podstaw SSP wg ICAO. Pozwoli to Państwu na ocenę istnienia i dojrzałości elementów SSP. Po wykonaniu i udokumentowaniu analizy luk, składniki/elementy zidentyfikowane jako brakujące lub niepełne wraz z istniejącymi stworzą podstawę planu wdrażania SSP.

2.2 Każdy składnik/element powinien zostać oceniony, aby ustalić, czy Państwo musi wydać lub zmodyfikować regulacje, polityki bądź procedury w celu ustanowienia wymaganych składników/elementów SSP. Podstawy SSP wg ICAO stanowiące podstawę do opracowania planu wdrażania SSP składają się z następujących czterech składników i jedenastu elementów:

1. Polityka i cele Państwa w zakresie bezpieczeństwa

   1.1 obowiązujące w Państwie przepisy dotyczące bezpieczeństwa;

   1.2 określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo;

   1.3 badanie wypadków i incydentów;

   1.4 polityka zapewniania przestrzegania przepisów.

2. Zarządzanie ryzykiem przez Państwo

   2.1 wymagania dotyczące SMS podmiotów lotniczych;

   2.2 uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych.

3. Zapewnianie bezpieczeństwa przez Państwo

   3.1 nadzór nad bezpieczeństwem;

   3.2 zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa;

   3.3 ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach.

2. Promowanie bezpieczeństwa przez Państwo

   4.1 wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa;

   4.2 zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

## 3. PLAN WDRAŻANIA SSP

3.1 Plan wdrażania SSP to projekt rozwoju SSP i zintegrowania go z innymi działaniami Państwa w obszarze zarządzania bezpieczeństwem. Z uwagi na to, że prawdopodobnie nakład pracy będzie ogromny, jest istotne, aby we właściwy sposób zarządzać obciążeniem pracą związaną z opracowywaniem i wdrażaniem SSP. Proponuje się, aby cztery składniki i jedenaście elementów podstaw SSP wg ICAO wdrażać w ustalonej kolejności, dającej możliwość osiągnięcia konkretnych rezultatów. Kolejność będzie zależeć od wyników analizy luk oraz złożoności i rozmiaru systemu lotniczego Państwa.

3.2 Jednym z celów SSP jest stworzenie otoczenia sprzyjającego wdrażaniu SMS przez podmioty lotnicze. Dlatego też wśród działań związanych z SSP cztery kroki wspierają wdrażanie SMS przez podmioty lotnicze. Kroki te omówione zostały w Rozdziale 11.

## 1. POLITYKA I CELE PAŃSTWA W ZAKRESIE BEZPIECZEŃSTWA

### 1.1 Obowiązujące w Państwie przepisy dotyczące bezpieczeństwa

a) Przegląd, opracowanie i wydanie (tam, gdzie to konieczne) krajowych ram legislacyjnych dotyczących bezpieczeństwa oraz specyficznych przepisów, zgodnie ze standardami międzynarodowymi i krajowymi, regulujących sposób, w jaki Państwo sprawuje nadzór nad zarządzaniem bezpieczeństwem w zakresie własnej jurysdykcji.

b) Ustanowienie grupy na szczeblu krajowym w formie rady, komitetu, etc. w celu zapewnienia skoordynowanego udziału instytucji lotniczych Państwa w konkretnych działaniach związanych z zarządzaniem bezpieczeństwem w Państwie oraz określenie ról, zakresów odpowiedzialności i powiązań pomiędzy tymi instytucjami.

c) Ustalenie harmonogramu okresowego przeglądu legislacji i przepisów operacyjnych w celu zapewnienia, że pozostają one odpowiednie i aktualne.

### 1.2 Określenie w ramach Państwa zakresów odpowiedzialności za bezpieczeństwo

a) Określenie, zdefiniowanie i udokumentowanie wymagań i zakresów odpowiedzialności za ustanowienie, i funkcjonowanie SSP. Obejmuje to wytyczne do planowania, organizowania, rozwijania, sprawowania kontroli oraz ciągłego ulepszania SSP w sposób realizujący cele Państwa w dziedzinie bezpieczeństwa. Dołączenie jasnej deklaracji dotyczącej przydzielenia zasobów koniecznych do wdrażania SSP.

b) Wskazanie i powołanie Dyrektora Odpowiedzialnego za SSP w Państwie, który powinien posiadać m.in.*:*

   1) ostateczną odpowiedzialność w imieniu Państwa za wdrożenie i funkcjonowanie SSP;

   2) pełnię władzy nad zasobami ludzkimi w instytucji lotniczej Państwa pełniącej najważniejszą rolę w SSP;

   3) pełnię władzy nad głównymi sprawami finansowymi w instytucji lotniczej Państwa pełniącej najważniejszą rolę w SSP;

   4) ostateczną władzę w sprawach związanych z zarządzaniem certyfikatami podmiotów lotniczych;

   5) ostateczną władzę nad rozwiązywaniem wszystkich problemów związanych z bezpieczeństwem w Państwie.

c) Powołanie zespołu wdrażającego SSP.

d) Ustalenie czasu potrzebnego na każde zadanie w ramach wdrażania SSP na różnych poziomach zarządzania w Państwowych instytucjach lotniczych.

e) Zapoznanie wszystkich pracowników na wszystkich szczeblach z koncepcją SSP, odpowiednio do zaangażowania w SSP.

f) Opracowanie i wdrożenie polityki Państwa w zakresie bezpieczeństwa zawierającej, ale niekoniecznie ograniczającej się do:

   1) zobowiązania do opracowywania i wdrażania strategii i procesów zapewniających, że wszelka działalność lotnicza pod nadzorem Państwa osiągnie najwyższy poziom bezpieczeństwa;

   2) opracowania i wydania krajowych podstaw prawnych w dziedzinie bezpieczeństwa i odpowiednich przepisów operacyjnych dotyczących zarządzania bezpieczeństwem w Państwie;

   3) zobowiązania do przekazania Państwowym instytucjom lotniczym zasobów koniecznych do wykonywania przez ich personel obowiązków, zarówno tych związanych z bezpieczeństwem, jak i pozostałych;

   4) wsparcia zarządzania bezpieczeństwem w Państwie poprzez skuteczny system zgłaszania i komunikowania zagrożeń;

5) ustanowienia rozwiązań służących ochronie systemów zbierania i przetwarzania danych dotyczących bezpieczeństwa (SDCPS);

6) zobowiązania do utrzymywania efektywnych interakcji z podmiotami lotniczymi przy rozwiązywaniu problemów związanych z bezpieczeństwem;

7) zobowiązania do przekazania polityki Państwa w zakresie bezpieczeństwa wszystkim pracownikom;

8) polityki zapewnienia przestrzegania przepisów uwzględniającej to, czy dany podmiot działa w środowisku SMS.

g) Ustanowienie koniecznych środków w celu zapewnienia, że polityka Państwa w zakresie bezpieczeństwa jest zrozumiana, wdrażana i przestrzegana na wszystkich poziomach w Państwowych instytucjach lotniczych.

**1.3 Badanie wypadków i incydentów**

a) Stworzenie mechanizmów zapewniających niezależne badanie wypadków i incydentów, którego jedynym celem jest zapobieganie wypadkom i incydentom, wspierając zarządzanie bezpieczeństwem w Państwie, a nie określanie winy lub odpowiedzialności.

b) Stworzenie rozwiązań koniecznych do zapewnienia niezależności instytucji badającej wypadki i incydenty od innych instytucji lotniczych Państwa.

**1.4 Polityka zapewnienia przestrzegania przepisów**

a) Stworzenie i wydanie polityki zapewnienia przestrzegania przepisów, określającej warunki i okoliczności, w których podmiotom lotniczym zezwala się na postępowanie wewnętrzne w sprawach niektórych zdarzeń, podczas których doszło do naruszeń warunków bezpieczeństwa, w kontekście systemu zarządzania bezpieczeństwem (SMS) danego podmiotu i za aprobatą właściwej władzy Państwowej. Polityka zapewnienia przestrzegania przepisów określa również warunki i okoliczności, w których mają zastosowanie procedury zapewnienia przestrzegania przepisów.

b) Polityka powinna również zapewniać, że żadne informacje uzyskane z wewnętrznych systemów zgłaszania zagrożenia i z systemów monitorowana lotów ustanowionych w ramach SMS nie będą użyte w celu zapewnienia przestrzegania przepisów.

**1.5 Dokumentacja SSP**

a) Założenie Państwowego archiwum bezpieczeństwa dokumentującego wymagania i zakresy odpowiedzialności w zakresie stworzenia i funkcjonowania SSP. Archiwum bezpieczeństwa będzie przechowywać i aktualizować dokumentację SSP związaną z obowiązującymi w Państwie przepisami dotyczącymi bezpieczeństwa, polityką i celami Państwa w zakresie bezpieczeństwa, wymagań SSP, procesów, procedur, zakresów odpowiedzialności i uprawnień oraz obowiązującego w Państwie akceptowalnego poziomu bezpieczeństwa (ALoS).

***Produkty***

1. Wydane krajowe przepisy dotyczące bezpieczeństwa.

2. Określone, udokumentowane i ogłoszone zakresy odpowiedzialności za bezpieczeństwo w Państwie.

3. Polityki bezpieczeństwa i zapewnienia przestrzegania przepisów w Państwie podpisane przez dyrektora odpowiedzialnego.

4. Polityki bezpieczeństwa i zapewnienia przestrzegania przepisów w Państwie rozpowszechnione wśród Państwowych instytucji lotniczych i nadzorowanych podmiotów lotniczych.

5. Ustanowiony niezależny proces badania wypadków i incydentów.

6. Ustanowiona struktura organizacyjna SSP.

***Etapy***

1. Wyznaczenie dyrektora odpowiedzialnego.

2. Opracowanie projektu polityki bezpieczeństwa.

3. Ustalenie zakresów i podziałów odpowiedzialności w dziedzinie bezpieczeństwa.

4. Zatwierdzenie zaproponowanej struktury organizacyjnej SSP.

5. Zatwierdzenie budżetu SSP.

*Uwaga.— W niniejszym Dodatku zaproponowano jedynie przykłady produktów i etapów. Możliwe są również inne produkty i etapy wdrażania składników SSP w Państwach o różnym zakresie i stopniu złożoności działalności lotniczej.*

## 2. ZARZĄDZANIE RYZYKIEM PRZEZ PAŃSTWO

### 2.1 Wymagania dotyczące SMS podmiotów lotniczych

a) Ustanowienie wymagań i konkretnych regulacji operacyjnych oraz polityki wdrażania SMS podmiotów lotniczych (ramy regulacyjne SMS, wytyczne, etc.) jako reguł określających, jak podmioty lotnicze będą identyfikować zagrożenia i zarządzać ryzykiem.

b) Ustanowienie harmonogramu konsultacji powyższych wymagań z podmiotami lotniczymi.

c) Ustanowienie harmonogramu okresowych przeglądów wymagań i konkretnych regulacji operacyjnych w celu zapewnienia, że pozostają one aktualne i odpowiednie dla podmiotów lotniczych.

### 2.2 Uzgadnianie warunków systemów zarządzania bezpieczeństwem podmiotów lotniczych

a) Opracowanie i ustanowienie procedury uzgadniania warunków bezpieczeństwa SMS indywidualnych podmiotów lotniczych w oparciu o:

1) wartości aktualnych wskaźników bezpieczeństwa;

2) wartości docelowych wskaźników bezpieczeństwa;

3) plany działania.

b) Uwzględnienie w uzgodnionej procedurze, że wyniki bezpieczeństwa podmiotu lotniczego powinny być współmierne do:

1) stopnia złożoności kontekstu operacyjnego danego podmiotu;

2) zasobów, którymi podmiot dysponuje w celu rozwiązywania problemów związanych z bezpieczeństwem.

c) Pomiary skuteczności SMS podmiotu lotniczego poprzez okresowe rewizje uzgodnionego poziomu bezpieczeństwa SMS w celu zapewnienia, że wskaźniki bezpieczeństwa pozostają aktualne i odpowiednie dla danego podmiotu.

d) Stworzenie sposobu oceny zdarzeń niższego rzędu i najczęstszych procesów w podmiotach lotniczych.

e) Określenie wymiernych wyników bezpieczeństwa dla różnych SMS.

***Produkty***

1. Wydane regulacje dotyczące SMS.

2. Wytyczne dotyczące wdrażania SMS rozpowszechnione wśród podmiotów lotniczych.

3. Wykonany pierwszy doroczny przegląd uzgodnionych warunków bezpieczeństwa podmiotów lotniczych.

***Etapy***

1. Przekazanie podmiotom lotniczym do konsultacji projektu regulacji dotyczących SMS.

2. Przekazanie podmiotom lotniczym do konsultacji projektu wytycznych dotyczących SMS.

3. Przeszkolenie personelu Państwowego w identyfikacji zdarzeń i zarządzania ryzykiem bezpieczeństwa.

4. Ukończenie procedury uzgadniania warunków bezpieczeństwa podmiotów lotniczych.

## 3. ZAPEWNIANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

### 3.1 Nadzór nad bezpieczeństwem

a) Ustanowienie mechanizmów gwarantujących, że identyfikacja zagrożeń i zarządzanie ryzykiem odbywa się według ustanowionych zasad.

b) Ustanowienie mechanizmu gwarantującego, że opcje kontroli ryzyka są włączone do SMS podmiotu lotniczego.

c) Ustanowienie wewnętrznego audytu SSP.

### 3.2 Zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa

a) Ustanowienie na poziomie Państwa środków zbierania, analizowania i przechowywania danych na temat zagrożeń i ryzyka:

   1) ustanowienie obowiązkowego systemu zgłaszania zagrożeń;

   2) ustanowienie poufnego systemu zgłaszania zagrożeń;

   3) stworzenie krajowej bazy danych o zagrożeniach;

   4) stworzenie mechanizmu generowania informacji z przechowywanych danych;

   5) stworzenie środków pozwalających na zbieranie danych o zagrożeniach zarówno w formie ogólnej na poziomie krajowym, jak i na poziomie indywidualnego podmiotu lotniczego;

   6) ustalenie środków pozwalających na wdrażanie planów naprawczych.

b) Zapewnienie, że procesy identyfikacji zagrożeń i zarządzania ryzykiem przez podmiot lotniczy są zgodne z wymaganiami, a opcje kontroli ryzyka są we właściwy sposób włączone do SMS podmiotu, choć niekoniecznie ograniczone do:

   1) inspekcji;

   2) audytów;

   3) ankiet.

c) Przestrzeganie następującej kolejności przy wdrażaniu:

1) wynikające z regulacji opcje kontroli ryzyka włączone do SMS podmiotu lotniczego;

2) działania nadzorcze w celu zapewnienia, że identyfikacja zagrożeń i zarządzanie ryzykiem przez podmiot lotniczy są zgodne z wymaganiami;

3) działania nadzorcze w celu sprawdzenia czy podmioty lotnicze stosują opcje kontroli ryzyka.

d) Ustanowienie akceptowalnego poziomu bezpieczeństwa (ALoS) w związku z SSP, zawierającego połączenie pomiaru bezpieczeństwa i pomiaru bezpieczeństwa operacyjnego:

1) Pomiar bezpieczeństwa zawiera w sobie kwantyfikację rezultatów zdarzeń poważnych z natury lub o poważnych konsekwencjach czy funkcji Państwa, np. współczynnik wypadków, współczynnik poważnych incydentów i zgodność z przepisami.

2) Pomiar bezpieczeństwa operacyjnego obejmuje kwantyfikację rezultatów procesów niskiego rzędu i o nieznacznych konsekwencjach, która pozwala mierzyć rzeczywiste wdrażanie SSP poza współczynnikiem wypadków i poziomem zgodności z przepisami.

### 3.3 Ukierunkowanie nadzoru, dzięki danym dotyczącym bezpieczeństwa, na obszary wymagające szczególnej uwagi i o największych potrzebach

a) Ustanowienie procedur priorytetów inspekcji, audytów i ankiet w oparciu o analizę zagrożeń i ryzyka.

***Produkty***

1. Wdrożony krajowy, obowiązkowy i poufny system zgłaszania zagrożeń.
2. Przeprowadzony pierwszy doroczny przegląd polityki i celów w zakresie bezpieczeństwa.
3. Przeprowadzony pierwszy doroczny przegląd polityki zapewniania przestrzeganie przepisów.
4. Określony ALoS.

***Etapy***

1. Zbieranie i przetwarzanie danych o zagrożeniach i ryzykach na poziomie krajowym.
2. Zbieranie informacji o zagrożeniach i ryzykach zarówno w formie zagregowanej na poziomie krajowym, jak i na poziomie indywidualnych podmiotów lotniczych.

## 4. PROMOWANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

### 4.1 Wewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa

a) Określenie potrzeb w zakresie szkoleń wewnętrznych.

b) Opracowanie podstawowego szkolenia w zakresie bezpieczeństwa i przeszkolenie całego personelu.

c) Opracowanie programu szkolenia z głównych składników SSP i SMS dla pracowników obejmującego:

1) wprowadzenie/wstępne szkolenie w zakresie bezpieczeństwa;

2) szkolenie na stanowisku pracy;

3) szkolenie przypominające.

d) Ustanowienie środków pomiaru skuteczności szkoleń.

e) Ustanowienie środków wewnętrznego komunikowania w sprawach związanych z bezpieczeństwem, w tym:

1) polityk i procedur;

2) newsletterów;

3) biuletynów;

4) strony internetowej.

**4.2 Zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa**

a) Ustanowienie środków dwustronnego komunikowania informacji istotnych dla bezpieczeństwa w celu wspierania wdrażania SMS przez podmioty lotnicze, w tym małych operatorów.

b) Opracowanie materiałów szkoleniowych i wytycznych dla podmiotów lotniczych na temat wdrażania SMS.

c) Ustanowienie środków komunikowania zewnętrznego w sprawach związanych z bezpieczeństwem, w tym:

1) polityki i procedur;

2) newsletterów;

3) biuletynów;

4) strony internetowej.

***Produkty***

1. Wykonany pierwszy cykl podstawowych szkoleń z bezpieczeństwa dla pracowników.

2. Opracowany program szkolenia na temat głównych składników SSP i SMS dla personelu technicznego i wsparcia.

3. Wytyczne na temat SMS rozpowszechnione wśród podmiotów lotniczych, w tym małych operatorów.

4. Wykonany pierwszy cykl szkoleń z wdrażania SMS dla podmiotów lotniczych.

5. Ustanowione środki wewnętrznego i zewnętrznego komunikowania informacji związanych z bezpieczeństwem.

***Etapy***

1. Ustanowienie wymagań dotyczących minimalnej wiedzy i doświadczenia dla personelu echnicznego wykonującego funkcje związane z nadzorem nad bezpieczeństwem.

2. Opracowanie i wydanie wytycznych poświęconych SMS.

3. Stworzenie programów szkolenia z SMS dla Państwowych instytucji lotniczych i podmiotów lotniczych.

4. Stworzenie krajowych newsletterów i biuletynów.

## Załącznik A

# SYSTEM ZGŁASZANIA INFORMACJI O WYPADKACH/INCYDENTACH ICAO (ADREP)

Zgodnie z Załącznikiem 13, *Badanie wypadków i incydentów statków powietrznych*, Państwa zgłaszają do ICAO informacje o wszystkich wypadkach z udziałem statków powietrznych o maksymalnej certyfikowanej masie startowej przekraczającej 2250 kg. ICAO zbiera również informacje o wszelkich incydentach z udziałem statków powietrznych powyżej 5700 kg. Ten system zawiadamiania znany jest jako ADREP. Państwa przesyłają określone dane w z góry ustalonym i zakodowanym formacie do ICAO. Przy odbiorze raportu ADREP, informacje są rejestrowane i gromadzone elektronicznie wchodząc w skład światowej bazy danych o zdarzeniach.

### PRZYKŁADOWA LISTA POWAŻNYCH INCYDENTÓW

Pojęcie „poważny incydent" zdefiniowane jest w rozdziale 1 Załącznika 13 następująco:

***Poważny incydent.*** Incydent, którego okoliczności zaistnienia wskazują, że nieomal doszło do wypadku.

Niżej opisane incydenty są typowymi przykładami tych, które można zaliczyć do kategorii poważnych. Wykaz ten nie jest wyczerpujący i służyć ma jedynie do zilustrowania określenia „poważny incydent".

- Niebezpieczne zbliżenie w trakcie którego, w celu uniknięcia zderzenia lub sytuacji niebezpiecznej, trzeba wykonać manewr zmiany kierunku (unik) lub kiedy celowe jest podjęcie zmiany kierunku.

- Sytuacja, w której ledwie udało się uniknąć zderzenia sprawnego statku powietrznego z ziemią.

- Przerwane starty z zamkniętej lub zajętej drogi startowej, z drogi kołowania[1] lub nieprzydzielonej drogi startowej.

- Starty z zamkniętej lub zajętej drogi startowej, z drogi kołowania lub nieprzydzielonej drogi startowej.

- Lądowania lub próba lądowania na zamkniętej lub zajętej drodze startowej, na drodze kołowania lub nieprzydzielonej drodze startowej.

- Wyraźna niezdolność osiągnięcia wymaganych parametrów podczas rozbiegu, podczas startu lub na początkowym odcinku nabierania wysokości.

- Pożary i przypadki pojawienia się dymu w kabinie pasażerskiej, przedziałach bagażowych lub pożary silnika, w tym pożary stłumione przy pomocy substancji gaśniczych.

- Sytuacje, w których członkowie załogi zostali zmuszeni do awaryjnego użycia instalacji tlenowej.

- Przypadki zniszczeń konstrukcji statku powietrznego lub uszkodzeń silnika, których nie można zakwalifikować do wypadków.

[1] Z wyjątkiem operacji śmigłowcowych po uzyskaniu zezwolenia.

- Niejednokrotna odmowa pracy jednego lub kilku systemów pokładowych, mających zasadnicze znaczenie dla eksploatacji statku powietrznego.

- Przypadki utraty zdolności do wykonywania czynności przez członków załogi statku powietrznego podczas lotu.

- Ilość paliwa wymagająca od pilota zgłoszenia o zaistnieniu sytuacji awaryjnej.

- Wtargnięcia na drogi startowe (Runway Incursions) klasyfikowane są jako zagrożenie A, zgodnie z Manual on the Prevention of Runway Incursions (Doc 9870), zawierającym informacje na temat klasyfikacji zagrożeń.

- Incydenty podczas startu lub lądowania, takie jak np. przyziemienie przed wyznaczonym punktem lub wytoczenie się poza granice drogi startowej.

- Odmowa pracy systemów, wejście w strefę niebezpiecznych zjawisk meteorologicznych, przekroczenia ustalonych ograniczeń lub inne sytuacje, które mogą spowodować utrudnienia w pilotowaniu statku powietrznego.

- Odmowa pracy więcej niż jednego systemu w układach rezerwowych, które są niezbędne do kierowania statkiem powietrznym.

## Załącznik B

# PLANOWANIE DZIAŁAŃ W SYTUACJACH KRYZYSOWYCH

### 1. WPROWADZENIE

1.1 Niewiele organizacji jest przygotowanych na wypadki lotnicze, być może dlatego, że zdarzają się one rzadko. Wiele organizacji nie ma skutecznych planów działania w sytuacjach nagłych lub kryzysowych. Funkcjonowanie organizacji po wypadku lub innej sytuacji nadzwyczajnej może zależeć od tego, jak poradziła sobie ona w pierwszych godzinach lub dniach po poważnym zdarzeniu związanym z bezpieczeństwem. Plan działań w sytuacjach kryzysowych opisuje, co należy zrobić po wypadku i kto jest odpowiedzialny za poszczególne działania. W operacjach lotniskowych plan działania w sytuacjach kryzysowych znany jest jako plan działań ratowniczych lotniska (AEP). W niniejszym podręczniku użyto ogólnego terminu plan działań kryzysowych (ERP).

1.2 O ile naturalnym jest kojarzenie planowania działań kryzysowych z operacjami statków powietrznych lub lotnisk, zazwyczaj w wyniku wypadku statku powietrznego, to koncepcja ta może być również zastosowana do innych podmiotów lotniczych. W przypadku służb ruchu lotniczego może to oznaczać wyłączenie zasilania, awarię radaru, utratę łączności lub innych ważnych urządzeń. Dla organizacji obsługowej może to być pożar hangaru lub znaczny wyciek paliwa. W tym kontekście sytuacja kryzysowa rozumiana jest jako wydarzenie mogące spowodować znaczne straty lub zakłócenia w działaniu organizacji.

1.3 Na pierwszy rzut oka planowanie działań kryzysowych może mieć niewiele wspólnego z zarządzaniem bezpieczeństwem. Jednakże skuteczne działania w sytuacji kryzysowej stanowią okazję do nauczenia się i zastosowania nabytej wiedzy w praktyce, co pozwoli zminimalizować straty lub obrażenia.

1.4 Sukces działań kryzysowych zaczyna się od prawidłowego planowania. Plan działań kryzysowych (ERP) stanowi podstawę systematycznego podejścia do zarządzania sprawami organizacji po znaczącym i nieplanowanym zdarzeniu – w najgorszym razie po poważnym wypadku.

1.5 Celem planu działań kryzysowych jest:

a) uporządkowane i wydajne przejście z trybu operacji normalnych na kryzysowe;

b) delegowanie uprawnień na czas sytuacji kryzysowej;

c) przydzielenie zadań kryzysowych;

d) zatwierdzenie przez kierownictwo działań zawartych w planie;

e) koordynacja działań podczas kryzysu;

f) bezpieczne kontynuowanie operacji lub jak najszybszy powrót do normalnych operacji.

### 2. WYMAGANIA ICAO

2.1 Każda organizacja prowadząca lub wspierająca operacje lotnicze powinna posiadać plan działań kryzysowych. Na przykład:

a) Załącznik 14 — *Lotniska* przewiduje, że lotnisko powinno posiadać lotniskowy plan działań ratowniczych współmierny do operacji statków powietrznych i innej działalności prowadzonej na lotnisku. Plan powinien obejmować koordynację działań w sytuacji kryzysowej na lotnisku lub w jego pobliżu.

b) Dokument *Przygotowanie podręcznika operacyjnego* (Doc 9376) wskazuje, że podręcznik operacyjny firmy powinien zawierać instrukcje i wytyczne co do obowiązków i zadań personelu po wypadku. Powinien też zawierać wytyczne co do powołania i funkcjonowania centrum kryzysowego – punktu kontaktowego w zakresie zarządzania kryzysowego. Wytyczne powinny odnosić się nie tylko do wypadków z udziałem statków powietrznych należących do firmy, ale również do wypadków z udziałem statków powietrznych, dla których jest ona agentem handlingowym (np. poprzez porozumienia code-share lub zamówione usługi). Większe firmy mogą zebrać wszystkie informacje dotyczące planowania kryzysowego w osobnym tomie podręcznika operacyjnego.

c) *Podręcznik służb lotniskowych* (Doc 9137), część 7 — *Planowanie kryzysowe na lotniskach* zawiera wytyczne zarówno dla władz lotniskowych, jak i przewoźników lotniczych w zakresie wstępnego planowania działań kryzysowych oraz koordynacji pomiędzy różnymi służbami lotniska, łącznie z operatorem.

2.2 W celu zapewnienia skuteczności, ERP powinien:

a) być odpowiednim i użytecznym dla osób, które mogą pełnić służbę w momencie wypadku;

b) zawierać listy kontrolne i łatwe do znalezienia dane kontaktowe właściwych pracowników;

c) być regularnie weryfikowanym poprzez ćwiczenia;

d) być uaktualnianym wraz ze zmianą szczegółowych informacji.

## 3. ZAWARTOŚĆ ERP

Plan działań kryzysowych (ERP) powinien mieć formę podręcznika. Powinien wskazywać zakresy odpowiedzialności, role i działania różnych agend i personelu zaangażowanego w działania kryzysowe. ERP powinien zawierać:

a) ***Właściwe przepisy i polityki.*** ERP powinien wskazywać właściwe przepisy, regulacje, porozumienia z władzami lokalnymi oraz polityki i priorytety firmy.

b) ***Postanowienia organizacyjne.*** ERP powinien przedstawiać intencje kierownictwa poprzez:

1) wskazanie, kto będzie kierował i kto będzie wyznaczony do zespołów działań kryzysowych;

2) określenie ról i odpowiedzialności pracowników wyznaczonych do zespołów kryzysowych;

3) wyjaśnienie zależności służbowych;

4) powołanie centrum zarządzania kryzysowego (CMC);

5) ustanowienie procedur w przypadku otrzymywania dużej liczby pytań i wniosków o informacje, zwłaszcza w pierwszych dniach po poważnym wypadku;

6) wyznaczenie rzecznika firmy do kontaktów z mediami;

7) określenie dostępnych zasobów, w tym upoważnień finansowych do nagłych działań;

8) wskazanie przedstawiciela firmy wobec wszelkich formalnych dochodzeń prowadzonych przez funkcjonariuszy Państwa;

9) ustalenie planu mobilizacji kluczowych pracowników itp.

Schemat organizacyjny powinien posłużyć do wskazania związków funkcyjnych i komunikacyjnych.

c) ***Notyfikacje.*** Plan powinien jasno wskazywać, kogo należy powiadomić w sytuacji nagłej i kto będzie powiadamiał osoby i instytucje spoza firmy i w jaki sposób. Należy uwzględnić następujące osoby/instytucje do powiadomienia:

1) kierownictwo;

2) władze Państwowe (poszukiwania i ratownictwo, regulator, komisja badania wypadków itp.);

3) lokalne służby ratownicze (władze portu lotniczego, straż pożarną, policję, pogotowie ratunkowe, instytucje medyczne itp.);

4) krewnych ofiar (jest to delikatna sprawa, którą w wielu Państwach zajmuje się policja);

5) pracowników firmy;

6) media;

7) dział prawny, księgowość, ubezpieczycieli itp.

d) ***Wstępna reakcja.*** Zależnie od okoliczności zespół początkowego reagowania może zostać wysłany na miejsce wypadku w celu wsparcia sił będących na miejscu i reprezentowania interesów firmy. Czynniki, które należy wziąć pod uwagę obejmują:

1) Kto ma kierować zespołem wstępnego reagowania?

2) Kto wejdzie w skład zespołu wstępnego reagowania?

3) Kto ma wypowiadać się w imieniu firmy na miejscu wypadku?

4) Co będzie potrzebne – specjalny sprzęt, ubrania, dokumentacja, środki transport, zakwaterowanie itp.?

e) ***Dodatkowa pomoc.*** Odpowiednio przeszkoleni i dysponujący doświadczeniem pracownicy mogą pomóc przy przygotowywaniu, ćwiczeniu i aktualizacji ERP organizacji. Wiedza ta może przydać się przy planowaniu i ćwiczeniu czynności takich jak:

1) odgrywanie roli pasażerów podczas ćwiczeń;

2) opieka nad tymi, którzy przeżyli wypadek;

3) kontakty z rodzinami itp.

f) ***Centrum zarządzania kryzysowego (CMC).*** CMC powinno zostać powołane w siedzibie organizacji, po spełnieniu początkowych kryteriów. Dodatkowo, na miejscu lub w pobliżu miejsca wypadku można utworzyć stanowisko dowodzenia (CP). ERP powinien określić sposób spełnienia następujących wymagań:

1) obsada personalna (być może 24 godziny dziennie, 7 dni w tygodniu, na początku działań kryzysowych);

2) środki łączności (telefony, fax, Internet itp.);

3) wymagana dokumentacja, prowadzenie rejestru czynności;

4) ochrona firmowych zbiorów informacji;

5) meble i wyposażenie biurowe;

6) dokumenty referencyjne (takie jak listy kontrolne i procedury działań kryzysowych, lotniskowe plany ratownictwa i listy kontaktów telefonicznych).

Usługi centrum zarządzania kryzysowego mogą być zlecone linii lotniczej lub wyspecjalizowanej organizacji w celu zadbania o interesy przewoźnika z dala od macierzystej bazy. Personel firmy powinien jak najszybciej przejąć zadania zlecone centrum kryzysowemu.

g) ***Zbiory danych.*** Poza potrzebą prowadzenia rejestrów czynności i zdarzeń, od organizacji będzie wymagane dostarczenie informacji Państwowym zespołom dochodzeniowym. Zespół reagowania kryzysowego powinien dostarczyć prowadzącym dochodzenie następujące informacje:

1) wszelkie dokumenty statku powietrznego, załogi i operacji;

2) listę punktów kontaktowych i wszelkiego personelu związanego ze zdarzeniem;

3) zapisy przesłuchań i oświadczeń wszystkich związanych ze zdarzeniem;

4) wszelkie dowody fotograficzne i inne.

h) ***Miejsce wypadku.*** Po poważnym wypadku przedstawiciele różnych instytucji mają prawo dostępu na miejsce zdarzenia, np. policja, straż pożarna, służby medyczne, władze lotniska, specjaliści medycyny sądowej, badający wypadek w imieniu Państwa, organizacje pomocowe takie jak Czerwony Krzyż, a nawet media. Chociaż koordynacja działań powyższych interesariuszy należy do policji i/lub Państwowej instytucji badającej wypadki, użytkownik statku powietrznego powinien zadbać o następujące aspekty działań na miejscu wypadku:

1) powołanie wyższego rangą przedstawiciela firmy na miejscu wypadku, również gdy wypadek miał miejsce:

— w bazie macierzystej;
— poza bazą macierzystą;
— na morzu lub za granicą.

2) postępowanie z pasażerami, którzy przeżyli;

3) potrzeby rodzin ofiar;

4) zabezpieczenie wraku;

5) zabezpieczenie szczątków ludzkich i rzeczy osobistych ofiar;

6) zabezpieczenie dowodów;

7) udzielenie pomocy władzom prowadzącym dochodzenie;

8) usunięcie i utylizacja wraku; itp.

i) ***Media informacyjne.*** To w jaki sposób firma kontaktuje się z mediami może mieć wpływ na to, jak szybko wróci ona do normalnego funkcjonowania po zdarzeniu. Konieczne są jasne wskazówki, np.:

1) które informacje są chronione prawem (zapisy FDR, CVR, kontroli ruchu lotniczego, zeznania świadków itp.);

2) kto może wypowiadać się w imieniu firmy w centrali i na miejscu wypadku (dyrektor public relations, prezes lub inny wyższy kierownik, zarządca, właściciel);

3) wskazówki dotyczące przygotowania oświadczenia jako natychmiastowej odpowiedzi na zapytania mediów;

4) co można przekazać mediom (czego należy unikać);

5) czas i zawartość pierwszego oświadczenia firmy;

6) regularne informowanie mediów.

j) ***Formalne dochodzenia.*** Należy wydać wytyczne dla pracowników firmy kontaktujących się z prowadzącymi dochodzenie w imieniu Państwa.

k) ***Pomoc rodzinom.*** EPR powinien również zawierać wskazówki co do podejścia firmy do zapewnienia pomocy rodzinom ofiar wypadku (załogi i pasażerów). Wskazówki mogą zawierać:

1) wymagania państwowe dotyczące świadczenia pomocy rodzinom;

2) rozwiązania dotyczące pomocy przy przejeździe i zakwaterowaniu na miejscu wypadku;

3) powołanie koordynatora i punktów kontaktowych dla każdej z rodzin;

4) dostarczanie aktualnych informacji;

5) pomoc psychologiczną itp.;

6) natychmiastową pomoc finansową dla rodzin i ofiar;

7) usługi pogrzebowe itp.

Niektóre Państwa określają rodzaje pomocy świadczonej przez przewoźnika.

l) ***Pomoc w radzeniu sobie ze stresem.*** ERP może zawierać wskazówki co do ograniczenia czasu pracy i zapewniania pomocy w radzeniu sobie ze stresem pracownikom pracującym w sytuacjach stresogennych.

m) ***Ewaluacja po zdarzeniu.*** Wskazówki powinny przewidywać, że kluczowy personel przeprowadzi debriefing i zanotuje wszelkie istotne informacje wyciągnięte ze zdarzenia, które mogą przyczynić się do wprowadzenia poprawek do ERP i związanych z nim list kontrolnych.

## 4. ZADANIA PRZEWOŹNIKA LOTNICZEGO

4.1 Plan działań kryzysowych (ERP) przewoźnika lotniczego powinien być skoordynowany z lotniskowym planem ratownictwa (AEP), aby pracownicy przewoźnika wiedzieli, za co odpowiada lotnisko, a co jest wymagane od przewoźnika. W ramach planowania działań kryzysowych przewoźnicy lotniczy powinni wspólnie z zarządzającymi lotniskami:

a) przeszkolić pracowników do działania w sytuacjach kryzysowych;

b) ustalić sposób postępowania z zapytaniami telefonicznymi w sprawie kryzysu;

c) określić dogodne miejsce oczekiwania dla osób, które nie odniosły obrażeń (witający i odwiedzający);

d) przekazać opis obowiązków pracowników firmy (np. osoby odpowiedzialnej, recepcjonistów przyjmujących pasażerów w miejscach oczekiwania);

e) zebrać podstawowe informacje o pasażerach i skoordynować sposób zaspokojenia ich potrzeb;

f) zawrzeć porozumienia o wzajemnej pomocy w sytuacjach kryzysowych z innymi przewoźnikami i agencjami;

g) przygotować i przechowywać zestaw kryzysowy zawierający:

1) konieczne wyposażenie administracyjne (formularze, papier, identyfikatory, komputery, itp.);

2) najważniejsze numery telefonów (lekarze, hotele w okolicy, tłumacze, firmy cateringowe, firmy świadczące usługi transportowe na rzecz linii lotniczych itp.).

4.2 W razie wypadku statku powietrznego na lotnisku lub w jego pobliżu, od przewoźników oczekuje się podjęcia działań takich jak:

a) zgłoszenie się do stanowiska kierowania w porcie lotniczym w celu skoordynowania działań użytkowników statków powietrznych;

b) pomoc przy zlokalizowaniu i odzyskaniu wszelkich rejestratorów lotu;

c) pomoc prowadzącym dochodzenie przy rozpoznaniu części statku powietrznego i zabezpieczeniu części niebezpiecznych;

d) dostarczenie informacji o pasażerach, załodze i ewentualnych materiałach niebezpiecznych na pokładzie;

e) przetransportowanie osób, które nie odniosły obrażeń do wyznaczonego miejsca oczekiwania;

f) obsługa osób, które nie odniosły obrażeń, a chcą kontynuować podróż lub potrzebują zakwaterowania lub innej pomocy;

g) przekazanie informacji mediom we współpracy z pracownikiem ds. informacji lotniska oraz policją;

h) usunięcie statku powietrznego/wraku za zgodą instytucji badającej wypadek.

Chociaż niniejszy akapit dotyczy wypadku statku powietrznego, niektóre z przedstawionych idei mogą być wykorzystane przy planowaniu kryzysowym zarządzających lotniskami i dostawców usług ruchu lotniczego.

## 5. LISTY KONTROLNE

Każdy zaangażowany w początkowe działania po poważnym wypadku będzie w pewnym stopniu przeżywał szok. Dlatego też proces reagowania w sytuacjach kryzysowych opiera się na listach kontrolnych. Listy te są integralną częścią podręcznika operacyjnego firmy lub podręcznika działań kryzysowych. Aby zachować użyteczność, listy kontrolne muszą być regularnie:

a) rewidowane i uaktualniane (np. aktualność listy mobilizacyjnej i danych kontaktowych);

b) przetestowane podczas realistycznych ćwiczeń.

## 6. SZKOLENIE I ĆWICZENIA

Plan działań kryzysowych jest deklaracją zamiarów na papierze. Najlepiej, żeby większa część ERP nie została nigdy przetestowana w prawdziwych okolicznościach. Szkolenie jest konieczne, aby intencje były poparte zdolnościami operacyjnymi. Ponieważ szkolenie ma krótki „termin przydatności” zaleca się regularne ćwiczenia. Pewne części ERP, takie jak mobilizacja, mogą być przećwiczone teoretycznie. Inne aspekty, takie jak działania „na miejscu” z udziałem innych agend, muszą być ćwiczone w regularnych odstępach. Zaletą tych ćwiczeń jest to, że ukazują słabości planu, które mogą zostać naprawione przed wystąpieniem rzeczywistego kryzysu.

## Załącznik C

# POWIĄZANE WYTYCZNE ICAO

### PODRĘCZNIKI

*Advanced Surface Movement Guidance and Control Systems (A-SMGCS) Manual* (Doc 9830)

*Aerodrome Design Manual* (Doc 9157)

*Airport Services Manual* (Doc 9137)

*Airworthiness Manual* (Doc 9760)

*Global Air Navigation Plan* (Doc 9750)

*Global Air Traffic Management Operational Concept* (Doc 9854)

*Human Factors Guidelines for Aircraft Maintenance Manual* (Doc 9824)

*Human Factors Guidelines for Air Traffic Management (ATM) Systems* (Doc 9758)

*Human Factors Guidelines for Safety Audits Manual* (Doc 9806)

*Human Factors Training Manual* (Doc 9683)

*Line Operations Safety Audit (LOSA)* (Doc 9803)

*Manual Concerning Interception of Civil Aircraft* (Doc 9433)

*Manual Concerning Safety Measures Relating to Military Activities Potentially Hazardous to Civil Aircraft Operations* (Doc 9554)

*Manual of Aircraft Accident and Incident Investigation* (Doc 9756)

Part I — *Organization and Planning*
Part III — *Investigation*[1]
Part IV — *Reporting*

*Manual of Aircraft Ground De-icing/Anti-icing Operations* (Doc 9640)

*Manual of All-Weather Operations* (Doc 9365)

*Manual of Civil Aviation Medicine* (Doc 8984)

*Manual of Procedures for Operations Inspection, Certification and Continued Surveillance (*Doc 8335)

*Manual of Radiotelephony* (Doc 9432)

*Manual on Airspace Planning Methodology for the Determination of Separation Minima* (Doc 9689)

*Manual on Air Traffic Management System Requirements* (Doc 9882)

*Manual on Certification of Aerodromes* (Doc 9774)

*Manual on Global Performance of the Air Navigation System* (Doc 9883)

*Manual on ICAO Bird Strike Information Systems (IBIS)* (Doc 9332)

*Manual on Implementation of a 300 m (1 000 ft) Reduced Vertical Separation Minimum Between FL 290 and FL 410 Inclusive* (Doc 9574)

*Manual on Required Communication Performance (RCP)* (Doc 9869)

*Manual on Simultaneous Operations on Parallel or Near-Parallel Instrument Runways (SOIR)* (Doc 9643)

---

[1] W przygotowaniu

*Manual of Surface Movement Guidance and Control Systems (SMGCS)* (Doc 9476)

*Normal Operations Safety Survey (NOSS)* (Doc 9910)

*Performance-based Navigation Manual* (Doc 9613)

*Preparation of an Operations Manual* (Doc 9376)

*Safety Oversight Audit Manual* (Doc 9735)

*Safety Oversight Manual* (Doc 9734)

**OKÓLNIKI**

*Assessment of ADS-B to Support Air Traffic Services and Guidelines for Implementation* (Cir 311)[1]

*A Unified Framework for Collision Risk Modelling in Support of the* Manual on Airspace Planning Methodology *with further applications* (Cir 319)

*Guidance on Assistance to Aircraft Accident Victims and Their Families* (Cir 285)

*Hazards at Aircraft Accident Sites* (Cir 315)

*Human Factors Digest No 15 — Human Factors in Cabin Safety* (Cir 300)

*Human Factors Digest No. 16 — Cross-cultural Factors in Aviation Safety* (Cir 302)

*Human Factors Digest No. 17 — Threat and Error Management (TEM) in Air Traffic Control* (Cir 314)

*Operation of New Larger Aeroplanes at Existing Aerodromes* (Cir 305)

*Training Guidelines for Aircraft Accident Investigators* (Cir 298)

**RÓŻNE**

Zawiadamianie ADREP (http://www.icao.int/anb/aig/Reporting.html)

**— KONIEC —**

[1] W przygotowaniu