

Warszawa, dnia 16 września 2020 r.

Poz. 48

**WYTYCZNE NR 13
PREZESA URZĘDU LOTNICTWA CYWILNEGO**

z dnia 16 września 2020 r.

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

Na podstawie art. 21 ust. 2 pkt 16 oraz art. 23 ust. 2 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2020 r. poz. 1580 i 1495 oraz z 2020 r. poz. 284 i 1378) ogłasza się, co następuje:

§ 1.1. W celu realizacji norm i zalecanych metod postępowania określonych w Załączniku 19 do Konwencji o międzynarodowym lotnictwie cywilnym, sporządzonej w Chicago dnia 7 grudnia 1944 r. (Dz. U. z 1959 r. poz. 212 i 214, z późn. zm.¹⁾) zaleca się stosowanie wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w Doc 9859 – „Podręcznik zarządzania bezpieczeństwem” (wydanie czwarte).

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

§ 2. Tracą moc wytyczne nr 13 Prezesa Urzędu Lotnictwa Cywilnego z dnia 10 grudnia 2015 r. w sprawie wprowadzenia do stosowania wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) – Doc 9859 (Dz. Urz. ULC poz. 66).

§ 3. Wytyczne wchodzą w życie z dniem ogłoszenia.

Prezes Urzędu Lotnictwa Cywilnego

Piotr Samson

¹⁾ Zmiany wymienionej umowy zostały ogłoszone w Dz. U. z 1963 r. poz. 137 i 138, z 1969 r. poz. 210 i 211, z 1976 r. poz. 130, 131, 188, 189, 227 i 228, z 1984 r. poz. 199 i 200, z 2000 r. poz. 446 i 447, z 2002 r. poz. 527 i 528, z 2003 r. poz. 700 i 701 oraz z 2012 r. poz. 368, 369, 370 i 371.



| ICAO

Doc 9859

Podręcznik zarządzania bezpieczeństwem

Wydanie czwarte, 2018 r.

Zatwierdzony i opublikowany pod nadzorem Sekretarza Generalnego

ORGANIZACJA MIĘDZYNARODOWEGO LOTNICTWA CYWILNEGO

Publikowane w osobnych wydaniach w języku angielskim, arabskim, chińskim, francuskim, rosyjskim i hiszpańskim przez
MIĘDZYNARODOWĄ ORGANIZACJĘ LOTNICTWA CYWILNEGO
999 Robert-Bourassa Boulevard, Montréal, Quebec, Kanada H3C 5H7

Informacje na temat zamawiania oraz pełna lista przedstawicieli handlowych i księgarń znajdują się na stronie ICAO pod adresem www.icao.int

Wydanie pierwsze, 2006

Wydanie trzecie, 2013

Wydanie czwarte, 2018

Doc 9859, Podręcznik Zarządzania Bezpieczeństwem

Numer zamówienia: 9859

ISBN 978-92-9258-552-5

© ICAO 2018

Wszelkie prawa zastrzeżone. Żadna część niniejszej publikacji nie może być powielana, przechowywana w systemie wyszukiwania ani przekazywana w jakiegokolwiek formie lub w jakikolwiek sposób bez uprzedniej pisemnej zgody Organizacji Międzynarodowego Lotnictwa Cywilnego.

PRZEDMOWA

Niniejsze czwarte wydanie Podręcznika zarządzania bezpieczeństwem (SMM) zastępuje w całości trzecie wydanie, opublikowane w maju 2013 r. Opracowanie niniejszego wydania zostało zapoczątkowane po przyjęciu Zmiany nr 1 do Załącznika 19 w celu uwzględnienia poprawek wprowadzonych przez zmianę oraz w celu odzwierciedlenia wiedzy i doświadczenia zdobytego od czasu ostatniego przeglądu podręcznika.

W celu uwzględnienia potrzeb zróżnicowanej społeczności lotniczej wdrażającej zarządzanie bezpieczeństwem oraz zalecenia drugiej Konferencji bezpieczeństwa wysokiego szczebla, która odbyła się w 2015 r., stworzono stronę internetową poświęconą wdrażaniu zarządzania bezpieczeństwem (SMI) (www.icao.int/SMI) mającą stanowić uzupełnienie Podręcznika zarządzania bezpieczeństwem, służącą jako repozytorium do udostępniania najlepszych praktyk. Na stronie tej będą na bieżąco gromadzone, przeglądane i publikowane praktyczne przykłady, narzędzia i pomocnicze materiały edukacyjne.



Niniejsze wydanie ma na celu wsparcie Państw we wdrażaniu skutecznych krajowych programów bezpieczeństwa (SSP). Oznacza to zapewnienie, że podmioty lotnicze wdrażają systemy zarządzania bezpieczeństwem (SMS) zgodnie z postanowieniami Załącznika 19. Aby zachować spójność z zasadami zarządzania bezpieczeństwem, podjęto wspólny wysiłek, aby skupić się na zamierzonym wyniku każdej normy i zalecanej metody postępowania (SARP), celowo unikając nadmiernego nakazywania. Nacisk położono na znaczenie każdej organizacji dostosowującej wdrożenie zarządzania bezpieczeństwem do swojego specyficznego środowiska.

Uwaga 1. – W niniejszym podręczniku termin „organizacja” odnosi się zarówno do Państw, jak i do podmiotów lotniczych.

Uwaga 2. – W niniejszym podręczniku termin „podmiot lotniczy” odnosi się do organizacji branży lotniczej wdrażającej system zarządzania bezpieczeństwem na zasadzie obowiązku lub dobrowolności, natomiast w Załączniku 19 termin ten jest stosowany w odniesieniu do bardzo szczegółowego wykazu organizacji znajdującego się w Rozdziale 3, który nie obejmuje międzynarodowych operatorów lotnictwa ogólnego.

Czwarte wydanie podzielone zostało na dziewięć rozdziałów, które stopniowo budują zrozumienie tematyki zarządzania bezpieczeństwem przez czytelnika. Rozdziały te można pogrupować według następujących trzech tematów:

- 1) *Podstawy zarządzania bezpieczeństwem* – Rozdziały od 1 do 3 budują zrozumienie przez czytelnika podstawowych zasad zarządzania bezpieczeństwem.
- 2) *Rozwój inteligencji w zakresie bezpieczeństwa* – Rozdziały od 4 do 7 bazują na podstawach. Rozdziały te zawierają cztery powiązane ze sobą tematy dotyczące wykorzystania danych oraz informacji dotyczących bezpieczeństwa do opracowania praktycznych informacji, które mogą być

wykorzystane przez kierownictwo organizacji do podejmowania decyzji w oparciu o dane, w tym decyzji dotyczących najbardziej efektywnego i skutecznego wykorzystania zasobów.

- 3) *Wdrożenie zarządzania bezpieczeństwem* – Rozdziały 8 i 9 wyjaśniają w jaki sposób stosować pojęcia z poprzedzających rozdziałów w celu instytucjonalizacji zarządzania bezpieczeństwem na poziomie Państwa i podmiotu lotniczego.

Niniejszy podręcznik nie zawiera wytycznych w zakresie norm i zalecanych metod postępowania dotyczących zarządzania bezpieczeństwem dla konkretnych sektorów będących poza zakresem Załącznika 19 (np. programy analizy danych o locie). *Podręcznik badania wypadków i incydentów lotniczych* (Doc 9756) zawiera wytyczne do prowadzenia niezależnych państwowych badań wypadków i incydentów zgodnie z Załącznikiem 13 - *Badanie wypadków i incydentów lotniczych*.

ICAO z wdzięcznością przyjmuje udział Zespołu ds. zarządzania bezpieczeństwem (SMP) oraz Grupy ds. wdrożenia ochrony informacji dotyczących bezpieczeństwa (SIP IG), jak również innych grup eksperckich i indywidualnych ekspertów, którzy zapewniali wsparcie, porady i wkład do niniejszego podręcznika. Treść została opracowana w okresie dwóch lat, a następnie została przedłożona do obszernego przeglądu w celu zebrania i uwzględnienia komentarzy ekspertów, mając na uwadze, że podręcznik ma zawierać kompleksowe wytyczne w zakresie zarządzania bezpieczeństwem dla szerokiej społeczności.

Uwagi dotyczące niniejszego podręcznika, szczególnie w odniesieniu do jego zastosowania i przydatności, przekazane przez wszystkie Państwa oraz w ramach działań kontrolnych w zakresie nadzoru nad bezpieczeństwem oraz działań w zakresie współpracy technicznej ICAO, będą mile widziane. Zostaną one uwzględnione podczas przygotowywania kolejnych wydań. Uwagi należy kierować na następujący adres:

The Secretary General
International Civil Aviation Organization
999 Robert-Bourassa Boulevard
Montréal, Quebec
Canada H3C 5H7

SPIS TREŚCI

	Strona
Słownik pojęć	vii
<i>Definicje</i>	<i>vii</i>
<i>Skróty i akronimy</i>	<i>ix</i>
Publikacje	xi
Rozdział 1 Wstęp	1-1
1.1. <i>Czym jest zarządzanie bezpieczeństwem?</i>	<i>1-1</i>
1.2. <i>Zastosowanie zarządzania bezpieczeństwem</i>	<i>1-3</i>
1.3. <i>Wdrożenie zarządzania bezpieczeństwem</i>	<i>1-5</i>
1.4. <i>Zintegrowane zarządzanie ryzykiem bezpieczeństwa</i>	<i>1-7</i>
Rozdział 2 Podstawy zarządzania bezpieczeństwem	2-1
2.1. <i>Koncepcja bezpieczeństwa i jego ewolucja</i>	<i>2-1</i>
2.2. <i>Ludzie w systemie</i>	<i>2-3</i>
2.3. <i>Związki przyczynowe wypadku</i>	<i>2-6</i>
2.4. <i>Dylemat zarządzania</i>	<i>2-9</i>
2.5. <i>Zarządzanie ryzykiem bezpieczeństwa</i>	<i>2-10</i>
Rozdział 3 Kultura bezpieczeństwa	3-1
3.1. <i>Wstęp</i>	<i>3-1</i>
3.2. <i>Kultura bezpieczeństwa i zarządzanie bezpieczeństwem</i>	<i>3-1</i>
3.3. <i>Tworzenie pozytywnej kultury bezpieczeństwa</i>	<i>3-3</i>
Rozdział 4 Zarządzanie poziomem bezpieczeństwa	4-1
4.1. <i>Wstęp</i>	<i>4-1</i>
4.2. <i>Cele bezpieczeństwa</i>	<i>4-3</i>
4.3. <i>Wskaźniki poziomu bezpieczeństwa (SPI) i cele poziomów bezpieczeństwa (SPT)</i>	<i>4-4</i>
4.4. <i>Monitorowanie poziomu bezpieczeństwa</i>	<i>4-12</i>
4.5. <i>Aktualizacja celów bezpieczeństwa</i>	<i>4-17</i>
Rozdział 5 Systemy zbierania i przetwarzania danych bezpieczeństwa	5-1
5.1. <i>Wstęp</i>	<i>5-1</i>
5.2. <i>Zbieranie danych bezpieczeństwa i informacji bezpieczeństwa</i>	<i>5-2</i>
5.3. <i>Taksonomie</i>	<i>5-8</i>
5.4. <i>Przetwarzanie danych bezpieczeństwa</i>	<i>5-10</i>
5.5. <i>Zarządzanie danymi bezpieczeństwa i informacjami bezpieczeństwa</i>	<i>5-12</i>
Rozdział 6 Analiza bezpieczeństwa	6-1
6.1. <i>Wstęp</i>	<i>6-1</i>
6.2. <i>Rodzaje analizy</i>	<i>6-2</i>
6.3. <i>Raportowanie wyników analizy</i>	<i>6-4</i>

6.4.	<i>Udostępnianie i wymiana informacji bezpieczeństwa</i>	6-5
6.5.	<i>Podjmowanie decyzji w oparciu o dane</i>	6-6
Rozdział 7 Ochrona danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł.....		7-1
7.1.	<i>Cele i treść</i>	7-1
7.2.	<i>Podstawowe zasady</i>	7-1
7.3.	<i>Zakres ochrony</i>	7-3
7.4.	<i>Poziom ochrony</i>	7-6
7.5.	<i>Zasady ochrony</i>	7-8
7.6.	<i>Zasady stosowania wyjątków</i>	7-11
7.7.	<i>Upublicznianie</i>	7-15
7.8.	<i>Ochrona zarejestrowanych danych</i>	7-17
7.9.	<i>Udostępnianie i wymiana informacji bezpieczeństwa</i>	7-17
Rozdział 8 Odpowiedzialność państwa za zarządzanie bezpieczeństwem		8-1
8.1.	<i>Wstęp</i>	8-1
8.2.	<i>Krajowy program bezpieczeństwa (SSP)</i>	8-2
8.3.	<i>Komponent nr 1: polityka bezpieczeństwa państwa, cele i zasoby</i>	8-4
8.4.	<i>Komponent nr 2: zarządzanie ryzykiem bezpieczeństwa przez państwo</i>	8-14
8.5.	<i>Komponent nr 3: zapewnienie bezpieczeństwa przez państwo</i>	8-22
8.6.	<i>Komponent nr 4: promowanie bezpieczeństwa przez państwo</i>	8-30
8.7.	<i>Wdrożenie krajowego programu bezpieczeństwa</i>	8-33
Rozdział 9 Systemy zarządzania bezpieczeństwem (SMS).....		9-1
9.1.	<i>Wstęp</i>	9-1
9.2.	<i>Struktura systemu zarządzania bezpieczeństwem</i>	9-1
9.3.	<i>Komponent nr 1: polityka bezpieczeństwa i jej cele</i>	9-2
9.4.	<i>Komponent nr 2: zarządzanie ryzykiem bezpieczeństwa</i>	9-10
9.5.	<i>Komponent nr 3: zapewnianie bezpieczeństwa</i>	9-18
9.6.	<i>Komponent nr 4: promowanie bezpieczeństwa</i>	9-25
9.7.	<i>Planowanie wdrożenia</i>	9-28

SŁOWNIK POJĘĆ

DEFINICJE

Jeżeli w podręczniku używane są następujące terminy, mają one znaczenia przedstawione poniżej.

Uwaga. - Jeżeli obok terminu pojawia się gwiazdka, oznacza to, że termin ten został już zdefiniowany w Załącznikach i Procedurach służb żeglugi powietrznej (PANS).

Akceptowalny poziom bezpieczeństwa (Acceptable level of safety performance - ALoSP). Poziom bezpieczeństwa uzgodniony przez władze Państwa, który ma zostać osiągnięty w lotnictwie cywilnym w danym Państwie, zdefiniowany w krajowym programie bezpieczeństwa, wyrażony w formie docelowych poziomów bezpieczeństwa i wskaźników poziomu bezpieczeństwa.

Dyrektor odpowiedzialny (Accountable executive). Pojedyncza, możliwa do zidentyfikowania osoba odpowiedzialna za skuteczne i wydajne działanie systemu zarządzania bezpieczeństwem (SMS) podmiotu lotniczego.

Zarządzanie zmianą (Change management). Formalny proces zarządzania zmianami w organizacji, prowadzony w sposób systematyczny, tak aby zmiany, które mogą mieć wpływ na zidentyfikowane zagrożenia i na strategie łagodzenia ryzyka, były uwzględniane zanim zostaną wdrożone.

Działania obronne (Defences). Konkretnie działania łagodzące, kontrole prewencyjne bądź sposoby odzyskiwania wprowadzone w celu zapobiegania wystąpieniu zagrożenia bądź jego eskalacji w niepożądany skutek.

Błędy (Errors). Działanie lub brak działania osoby w pionie operacyjnym, które prowadzi do odejścia od organizacyjnych lub operacyjnych intencji lub oczekiwań tej osoby.

***Zagrożenie (Hazard).** Stan lub obiekt, który może spowodować lub przyczynić się do incydentu lub wypadku lotniczego.

Łagodzenie ryzyka (Risk mitigation). Proces obejmujący działania obronne, kontrole prewencyjne lub sposoby odzyskiwania mający na celu zmniejszenie dotkliwości i/lub prawdopodobieństwa przewidywanych konsekwencji zagrożenia.

Bezpieczeństwo (Safety). Stan, w którym ryzyka związane z różnymi rodzajami działalności lotniczej, związanymi lub stanowiącymi bezpośrednie wsparcie operacji statku powietrznego, są obniżone do akceptowalnego poziomu i kontrolowane.

***Dane bezpieczeństwa (Safety data).** Zdefiniowany zestaw faktów lub wartości dotyczących bezpieczeństwa zebranych z różnych źródeł związanych z lotnictwem, który służy do utrzymania lub poprawy bezpieczeństwa.

Uwaga. – Dane bezpieczeństwa są zbierane z obszaru proaktywnych lub reaktywnych działań związanych z bezpieczeństwem, w tym między innymi:

- a) badań wypadków lub incydentów;
- b) zgłoszeń dotyczących bezpieczeństwa;
- c) zgłoszeń dotyczących ciągłej zdatności do lotu;
- d) monitorowania działań operacyjnych;
- e) inspekcji, audytów, ankiet; lub
- f) badań i przeglądów bezpieczeństwa.

***Informacje bezpieczeństwa (Safety information).** Dane bezpieczeństwa, które są przetwarzane, organizowane lub analizowane w danym kontekście, tak aby były użyteczne dla celów zarządzania bezpieczeństwem.

***System Zarządzania Bezpieczeństwem (Safety management system (SMS)).** Systematyczne podejście do zarządzania bezpieczeństwem obejmujące niezbędne struktury organizacyjne, zakres odpowiedzialności, zakres obowiązków, politykę oraz procedury.

Cel bezpieczeństwa (Safety objective). Krótkie oświadczenie wysokiego szczebla dotyczące osiągnięć w zakresie bezpieczeństwa lub pożądanego rezultatu, który ma być uzyskany w wyniku wdrożenia krajowego programu bezpieczeństwa lub systemu zarządzania bezpieczeństwem podmiotu lotniczego.

Uwaga. – Cele bezpieczeństwa są opracowywane na podstawie najwyższych ryzyk dotyczących bezpieczeństwa organizacji i powinny być brane pod uwagę podczas późniejszego opracowywania wskaźników poziomu bezpieczeństwa i celów poziomu bezpieczeństwa.

***Nadzór nad bezpieczeństwem (Safety oversight).** Funkcja wykonywana przez Państwo mająca na celu zapewnienie, że osoby fizyczne i organizacje wykonujące działalność lotniczą przestrzegają krajowe przepisy i regulacje dotyczące bezpieczeństwa.

***Poziom bezpieczeństwa (Safety performance).** Osiągnięcie w zakresie bezpieczeństwa Państwa lub podmiotu lotniczego zdefiniowane przez cele poziomu bezpieczeństwa i wskaźniki poziomu bezpieczeństwa.

***Wskaźnik poziomu bezpieczeństwa (Safety performance indicator).** Parametr oparty na danych, używany do monitorowania i oceny poziomu bezpieczeństwa.

***Cel poziomu bezpieczeństwa (Safety performance target).** Planowana lub zamierzona przez Państwo lub podmiot lotniczy, w danym przedziale czasowym, wartość celu wskaźnika poziomu bezpieczeństwa, która jest zgodna z celem bezpieczeństwa.

***Ryzyko bezpieczeństwa (Safety risk).** Przewidywane prawdopodobieństwo i dotkliwość konsekwencji lub skutków zagrożenia.

***Krajowy program bezpieczeństwa (State Safety Programme (SSP)).** Zintegrowany zestaw działań i przepisów mających na celu poprawę bezpieczeństwa.

***Nadzór (Surveillance).** Działania Państwa, w ramach których Państwo w sposób proaktywny weryfikuje poprzez inspekcje i audyty, że posiadacze licencji, certyfikatów, upoważnień lub zatwierdzeń lotniczych nieprzerwanie spełniają ustanowione wymagania oraz funkcjonują na poziomie kompetencji i bezpieczeństwa wymaganym przez Państwo.

System (System). Zorganizowana, celowa struktura składająca się ze wzajemnie powiązanych i współzależnych elementów i komponentów oraz powiązanych polityk, procedur i praktyk stworzona w celu prowadzenia określonej działalności lub rozwiązania problemu.

Czynnik uruchamiający (Trigger). Ustalony poziom lub wartość kryteriów dla konkretnego wskaźnika poziomu bezpieczeństwa, który służy do zainicjowania wymaganego działania (np. oceny, korekty lub działania naprawczego).

SKRÓTY I AKRONIMY

ADREP	Accident/incident data reporting	System przekazywania danych o wypadkach i incydentach
AIA	Accident investigation authority	Organ uprawniony do badania wypadku
ALoSP	Acceptable level of safety performance	Akceptowalny poziom bezpieczeństwa
AOC	Air operator certificate	Certyfikat przewoźnika lotniczego
ATS	Air traffic services	Służby ruchu lotniczego
CAA	Civil aviation authority	Organ lotnictwa cywilnego
CVR	Cockpit voice recorder	Pokładowy rejestrator rozmów w kabinie pilota
D3M	Data-driven decision-making	Podjęcie decyzji w oparciu o dane
Doc	Document	Dokument
ERP	Emergency response plan	Plan reagowania awaryjnego
FDA	Flight data analysis	Analiza danych o locie
FDR	Flight data recorder	Rejestrator parametrów lotu
FMS	Financial management system	System zarządzania finansowego
FRMS	Fatigue risk management systems	Systemy zarządzania ryzykiem związanym ze zmęczeniem
GASP	Global Aviation Safety Plan	Globalny plan bezpieczeństwa lotniczego
ICAO	International Civil Aviation Organization	Organizacja Międzynarodowego Lotnictwa Cywilnego
iSTARs	Integrated Safety Trend Analysis and Reporting System	Zintegrowany system analizy i zgłaszania trendów dotyczących bezpieczeństwa
LOSA	Line operations safety audit	Audyt bezpieczeństwa operacji liniowych
OHSMS	Occupational health and safety management system	System zarządzania bezpieczeństwem i higieną pracy
OSHE	Occupational safety, health and environment	Bezpieczeństwo i higiena pracy
PIRG	Planning and implementation regional group	Regionalna grupa ds. planowania i wdrożenia
QMS	Quality management system	System zarządzania jakością
RASG	Regional aviation safety group	Regionalna grupa ds. bezpieczeństwa lotniczego
RSOO	Regional Safety Oversight Organization	Regionalna organizacja nadzoru nad bezpieczeństwem
SAG	Safety action group	Grupa ds. działań związanych z bezpieczeństwem
SARPs	Standards and Recommended Practices	Normy i zalecane metody postępowania
SD	Standard deviation	Odchylenie standardowe
SDCPS	Safety data collection and processing systems	Systemy zbierania i przetwarzania danych dotyczących bezpieczeństwa
SeMS	Security management system	System zarządzania ochroną
SMM	Safety management manual	Podręcznik zarządzania bezpieczeństwem
SMP	Safety management panel	Zespół ds. zarządzania bezpieczeństwem
SPI	Safety performance indicator	Wskaźnik poziomu bezpieczeństwa
SPT	Safety performance target	Cel poziomu bezpieczeństwa
SRB	Safety review board	Komisja ds. przeglądu bezpieczeństwa
SRBS	Safety risk-based surveillance	Nadzór w oparciu o ryzyko bezpieczeństwa
SRM	Safety risk management	Zarządzanie ryzykiem bezpieczeństwa
SSO	State safety oversight	Krajowy nadzór nad bezpieczeństwem
SSP	State safety programme	Krajowy program bezpieczeństwa
STDEVP	Population standard deviation	Odchylenie standardowe w populacji
TNA	Training needs analysis	Analiza potrzeb szkoleniowych
USOAP	Universal Safety Oversight Audit Programme	Globalny program kontroli nadzoru nad bezpieczeństwem ICAO

PUBLIKACJE

(o których mowa w niniejszym podręczniku)

Poniższe dokumenty zostały przywołane w niniejszym podręczniku lub mogą stanowić dodatkowe materiały zawierające wytyczne.

DOKUMENTY ICAO

Załączniki do Konwencji o międzynarodowym lotnictwie cywilnym

Załącznik 1 — *Licencjonowanie personelu*

Załącznik 6 — *Eksploatacja statków powietrznych*

Część I — *Międzynarodowy zarobkowy transport lotniczy — Samoloty*

Część II — *Międzynarodowe lotnictwo ogólne – Samoloty*

Załącznik 8 — *Zdatność do lotu statków powietrznych*

Załącznik 13 — *Badanie wypadków i incydentów lotniczych*

Załącznik 14 — *Lotniska*

Tom I — *Projektowanie i eksploatacja lotnisk*

Załącznik 18 – *Bezpieczny transport materiałów niebezpiecznych drogą powietrzną*

Załącznik 19 – *Zarządzanie bezpieczeństwem*

PANS

Procedury służb żeglugi powietrznej (PANS) – Lotniska (Doc 9981)

Procedury służb żeglugi powietrznej – Zarządzanie ruchem lotniczym (PANS-ATM, Doc 4444)

PODRĘCZNIKI

Podręcznik służb portu lotniczego (Doc 9137)

Część 3 – *Kontrola i ograniczanie obecności zwierząt*

Podręcznik planowania służb ruchu lotniczego (Doc 9426)

Podręcznik zdatności do lotu (Doc 9760)

Podręcznik ochrony w lotnictwie (Doc 8973 – Wydanie zastrzeżone)

Globalny plan bezpieczeństwa lotniczego (ang. Global Aviation Safety Plan - GASP) (Doc 10004)

Podręcznik badania wypadków i incydentów lotniczych (Doc 9756)

Część I – Organizacja i planowanie

Część II – Procedury i listy kontrolne

Część III – Badanie

Część IV – Raportowanie

Podręcznik nadzoru nad podejściami do zarządzania zmęczeniem (Doc 9966)

Podręcznik emiterów laserowych i bezpieczeństwa lotu (Doc 9815)

Podręcznik systemów bezzałogowych statków powietrznych (RPAS) (Doc 10019)

Podręcznik kompetencji inspektorów bezpieczeństwa lotnictwa cywilnego (Doc 10070)

Podręcznik systemu informacji o zderzeniach z ptakami ICAO (IBIS) (Doc 9332)

Podręcznik ochrony informacji dotyczących bezpieczeństwa (Doc 10053)

Część I – Ochrona rejestrów dotyczących badań wypadków i incydentów

Podręcznik nadzoru nad bezpieczeństwem (Doc 9734)

Część A — Ustanowienie i zarządzanie krajowym systemem nadzoru nad bezpieczeństwem

Część B – Ustanowienie i zarządzanie regionalną organizacją nadzoru nad bezpieczeństwem

Instrukcje techniczne bezpiecznego transportu materiałów niebezpiecznych drogą powietrzną (Doc 9284)

ROZDZIAŁ 1

WSTĘP

1.1. CZYM JEST ZARZĄDZANIE BEZPIECZEŃSTWEM?

1.1.1. Zarządzanie bezpieczeństwem ma na celu proaktywne ograniczanie ryzyk bezpieczeństwa, zanim spowodują one wypadki i incydenty lotnicze. Dzięki wdrożeniu zarządzania bezpieczeństwem Państwa mogą zarządzać swoimi działaniami w zakresie bezpieczeństwa w bardziej zdyscyplinowany, zintegrowany i skoncentrowany sposób. Jednoznaczne rozumienie jego roli i udziału w bezpiecznych operacjach umożliwia Państwu i jego branży lotniczej określenie priorytetów działań mających na celu przeciwdziałanie ryzykom bezpieczeństwa i skuteczniejsze zarządzanie swoimi zasobami dla osiągnięcia optymalnych korzyści związanych z bezpieczeństwem lotniczym.

1.1.2. Skuteczność działań Państwa w zakresie zarządzania bezpieczeństwem jest wzmocniona kiedy działania wdrażane są w sposób formalny i zinstytucjonalizowany poprzez krajowy program bezpieczeństwa (SSP) oraz poprzez systemy zarządzania bezpieczeństwem (SMS) podmiotów lotniczych. Krajowy program bezpieczeństwa, w połączeniu z systemami SMS podmiotów lotniczych, w sposób systematyczny uwzględnia ryzyka bezpieczeństwa, poprawia poziom bezpieczeństwa każdego podmiotu lotniczego oraz zbiorczo poprawia poziom bezpieczeństwa Państwa.

1.1.3. Krajowy program bezpieczeństwa (SSP) jest opracowywany i utrzymywany przez każde Państwo jako ustrukturyzowane podejście mające na celu wsparcie w zarządzaniu bezpieczeństwem lotniczym. Istniejący rejestr bezpieczeństwa lotniczego został osiągnięty dzięki tradycyjnemu podejściu w oparciu o zgodność i powinien być nadal traktowany jako podstawa SSP. W związku z tym Państwa powinny zapewnić posiadanie skutecznych systemów nadzoru nad bezpieczeństwem. Więcej informacji na temat krajowego programu bezpieczeństwa znajduje się w Rozdziale 8.

1.1.4. Państwa wymagają, aby podmioty lotnicze będące pod ich jurysdykcją, wdrożyły system zarządzania bezpieczeństwem, jak określono w Załączniku 19 - *Zarządzanie bezpieczeństwem*, w celu ciągłego podnoszenia poziomu bezpieczeństwa poprzez identyfikację zagrożeń, gromadzenie i analizowanie danych oraz ciągłą ocenę i zarządzanie ryzykami bezpieczeństwa (patrz pkt 1.2 w zakresie szczegółowych informacji dotyczących zastosowania SMS). Więcej informacji na temat wdrożenia systemu zarządzania bezpieczeństwem znajduje się w Rozdziale 9.

1.1.5. Cele *Globalnego planu bezpieczeństwa lotniczego ICAO* (GASP, Doc 10004) wymagają od Państw wdrożenia solidnych i zrównoważonych systemów nadzoru nad bezpieczeństwem oraz stopniowego przekształcania ich w bardziej zaawansowane środki zarządzania poziomem bezpieczeństwa. Cele te są zgodne z wymaganiami ICAO dotyczącymi wdrożenia krajowych programów bezpieczeństwa oraz systemów zarządzania bezpieczeństwem przez podmioty prowadzące działalność w lotnictwie cywilnym.

1.1.6. Podejście w oparciu o poziom bezpieczeństwa daje możliwość doskonalenia, ponieważ koncentruje się na osiągnięciu pożądanego rezultatu, a nie wyłącznie na tym, czy dane Państwo zachowuje zgodność, czy też nie. Należy jednak zauważyć, że wdrożenie takiego podejścia oparte jest na współpracy, ponieważ wymaga wysiłku ze strony branży lotniczej w opracowaniu odpowiednich środków do osiągnięcia określonych wyników, a ze strony Państw w ocenie podejścia każdego podmiotu lotniczego.

1.1.7. KORZYŚCI WYNIKAJĄCE Z ZARZĄDZANIA BEZPIECZEŃSTWEM

Wdrożenie zarządzania bezpieczeństwem przynosi wiele korzyści, spośród których niektóre obejmują elementy:

- a) *Wzmocniona kultura bezpieczeństwa* – kultura bezpieczeństwa organizacji może zostać wzmocniona poprzez uwidocznienie zaangażowania kierownictwa oraz poprzez aktywny udział personelu w zarządzaniu ryzykiem bezpieczeństwa. Kiedy kierownictwo popiera bezpieczeństwo wskazując je jako priorytet, jest to zazwyczaj dobrze przyjmowane przez personel i staje się częścią normalnych operacji.
- b) *Udokumentowane, oparte na procesie podejście mające na celu zapewnienie bezpieczeństwa* – ustanawia jasne i udokumentowane podejście do osiągnięcia bezpiecznych operacji, które jest zrozumiałe dla personelu i może być w łatwy sposób wyjaśnione innym osobom. Ponadto jasne zdefiniowanie podstawowego działania umożliwi wprowadzanie zmian w sposób kontrolowany, przy ciągłym doskonaleniu programu/systemu bezpieczeństwa, pomagając w ten sposób organizacji optymalizować zasoby wymagane do wdrożenia zmian.
- c) *Lepsze zrozumienie interfejsów i relacji związanych z bezpieczeństwem* – proces dokumentowania i definiowania interfejsów zarządzania bezpieczeństwem może przynieść korzyści w postaci zrozumienia relacji pomiędzy procesami w organizacji, prowadząc do lepszego zrozumienia całego procesu i wyeksponowania możliwości zwiększenia wydajności.
- d) *Lepsze wczesne wykrywanie zagrożeń bezpieczeństwa* – poprawia zdolność Państwa/podmiotu prowadzącego działalność w lotnictwie cywilnym do wykrywania pojawiających się problemów związanych z bezpieczeństwem, które mogą zapobiegać wypadkom i incydentom dzięki proaktywnej identyfikacji zagrożeń i zarządzaniu ryzykami bezpieczeństwa.
- e) *Podejmowanie decyzji w oparciu o dane bezpieczeństwa* – poprawia zdolność Państwa/podmiotu wykonującego działalność w lotnictwie cywilnym do gromadzenia danych dotyczących bezpieczeństwa do celów analizy bezpieczeństwa. Dzięki strategicznemu myśleniu w celu określenia pytań, na które należy udzielić odpowiedzi, wynikające z tego informacje bezpieczeństwa mogą pomóc decydentom, w czasie zbliżonym do rzeczywistego, w podejmowaniu trafniejszych decyzji. Ważnym aspektem tego procesu decyzyjnego jest przydział zasobów do obszarów budzących większe obawy lub wymagających wsparcia.
- f) *Lepsza komunikacja w zakresie bezpieczeństwa* – zapewnia wspólny język w zakresie bezpieczeństwa w całej organizacji i branży. Wspólny język w zakresie bezpieczeństwa stanowi kluczowy czynnik umożliwiający wspólne zrozumienie celów i osiągnięć bezpieczeństwa organizacji. W szczególności zapewnia uznanie celów bezpieczeństwa organizacji, jej wskaźników poziomu bezpieczeństwa (SPI) oraz docelowych poziomów bezpieczeństwa (SPT), które zapewniają kierunek i motywację dla bezpieczeństwa. Personel będzie bardziej świadomy działań organizacji oraz postępów w osiąganiu zdefiniowanych celów bezpieczeństwa, a także sposobu, w jaki przyczyniają się one do sukcesu organizacji. Wspólny język w zakresie bezpieczeństwa umożliwi podmiotom lotniczym z wieloma rodzajami lotniczej działalności gromadzenie informacji bezpieczeństwa we wszystkich jednostkach organizacyjnych. Wsparcie zarządzania interfejsami jest niezbędne w całym systemie lotniczym.
- g) *Dowód, że bezpieczeństwo stanowi priorytet* – pokazuje w jaki sposób kierownictwo wspiera i zapewnia bezpieczeństwo, w jaki sposób ryzyka bezpieczeństwa są identyfikowane i zarządzane, a także w jaki sposób poziom bezpieczeństwa jest stale poprawiany, powodując zwiększenie zaufania wśród społeczności lotniczej, wewnątrz i na zewnątrz organizacji. Powoduje to również, że personel ma pewność co do poziomu bezpieczeństwa organizacji, co może prowadzić do zwiększonej atrakcyjności pracy i utrzymania wysokiego poziomu pracowników. Pozwala także Państwu i regionalnym organizacjom nadzoru nad bezpieczeństwem (RSOO) zdobyć zaufanie co do poziomu bezpieczeństwa podmiotów lotniczych.
- h) *Ewentualne oszczędności finansowe* – mogą pozwolić niektórym podmiotom prowadzącym działalność w lotnictwie cywilnym na uzyskanie zniżek na swoje składki ubezpieczeniowe i/lub

obniżenie składek na ubezpieczenie pracowników w oparciu o wyniki działania systemu zarządzania bezpieczeństwem.

- i) *Poprawiona wydajność* – możliwe zmniejszenie kosztów operacji poprzez wyeksponowanie braku wydajności w istniejących procesach i systemach. Integracja z innymi wewnętrznymi lub zewnętrznymi systemami zarządzania może również zaoszczędzić na dodatkowych kosztach.
- j) *Unikanie kosztów* – poprzez proaktywną identyfikację zagrożeń i zarządzanie ryzykiem bezpieczeństwa (SRM), kosztów związanych z wypadkami i incydentami można uniknąć. W takich przypadkach koszty bezpośrednie mogą obejmować: obrażenia, uszkodzenie mienia, naprawy sprzętu i opóźnienia w harmonogramie. Koszty pośrednie mogą obejmować: działania prawne; utratę biznesu i utratę reputacji, nadwyżki części zamiennych, narzędzia i szkolenia, zwiększone składki ubezpieczeniowe, utratę produktywności personelu, odzyskiwanie sprzętu i sprzątnięcie, utratę użytkowania sprzętu prowadzącą do krótkoterminowego wykorzystania sprzętu zastępczego oraz wewnętrzne dochodzenia.

1.2. ZASTOSOWANIE ZARZĄDZANIA BEZPIECZEŃSTWEM

Odpowiedzialność Państwa za zarządzanie bezpieczeństwem została omówiona w Załączniku 19, Rozdział 3, i obejmuje wymóg wdrożenia systemu zarządzania bezpieczeństwem przez podmioty lotnicze określone w SARP. Przepisy dotyczące wdrożenia systemów zarządzania bezpieczeństwem przez podmioty lotnicze znajdują się w Rozdziale 4 oraz w Dodatku 2 Załącznika 19.

1.2.1 Zastosowanie systemu zarządzania bezpieczeństwem (SMS)

1.2.1.1 Ocena mająca na celu określenie możliwości zastosowania SMS do Zmiany nr 1 do Załącznika 19 opiera się na zestawie kryteriów. Oczekuje się, że te same kryteria będą okresowo wykorzystywane przez ICAO i Zespół ds. zarządzania bezpieczeństwem (SMP) przy ponownej ocenie potrzeby rozszerzenia zastosowania na inne organizacje lotnicze.

Kompleksowe podejście systemowe do bezpieczeństwa

1.2.1.2 Kompleksowe podejście systemowe do bezpieczeństwa uznaje całą branżę lotniczą za system. Wszystkie podmioty lotnicze oraz ich systemy zarządzania bezpieczeństwem są uważane za podsystemy. Dzięki temu Państwo może rozważyć interakcje, oraz przyczynę i skutek, w całym systemie. Budowanie systemów bezpieczeństwa w ten sam sposób jest często niemożliwe lub niepraktyczne. Dlatego główną obawę Państw i podmiotów lotniczych stanowi jak najlepszy sposób zarządzania interfejsami między różnymi wzajemnie na siebie oddziałującymi systemami.

1.2.1.3 Podczas oceny zastosowania SMS uwzględniono powiązanie między podmiotami lotniczymi, które posiadają SMS zgodnie z wymaganiami Załącznika 19, a innymi organizacjami prowadzącymi działalność lotniczą. Zastosowanie SMS powinno zmniejszyć ryzyko luk lub nakładania się, i nie powinno zwiększać ryzyka bezpieczeństwa poprzez zmniejszenie interoperacyjności.

Konsekwencje podwykonawstwa

1.2.1.4 Aby zarządzanie ryzykiem bezpieczeństwa (SRM) było skuteczne w odniesieniu do wszystkich podmiotów lotniczych, ważne jest jasne określenie obowiązków związanych z identyfikacją zagrożeń oraz zarządzaniem ryzykami bezpieczeństwa dla całego łańcucha usług w systemie, bez luk lub nakładania się. Jeżeli podmiot lotniczy, którego dotyczy wymóg wdrożenia SMS, podpisuje umowę z organizacją, która nie podlega wymogowi wdrożenia SMS, zagrożenia oraz ryzyka bezpieczeństwa potencjalnie wprowadzone przez wykonawcę są uwzględniane w ramach SMS podmiotu lotniczego. To nakłada na podmiot dodatkowe obowiązki związane z SRM polegające na zapewnieniu wiedzy na temat ryzyk spowodowanych działaniami jego kontrahenta(-ów). Więcej informacji na temat zarządzania ryzykiem bezpieczeństwa znajduje się w Rozdziale 2.

Kontrola ryzyka bezpieczeństwa za pomocą przepisów

1.2.1.5 Państwa powinny ocenić, czy istniejące przepisy i regulacje skutecznie odnoszą się do zagrożeń związanych z daną działalnością. Może się zdarzyć, że istniejące wymogi zapewniają wystarczające środki łagodzenia ryzyka bezpieczeństwa, a nałożenie wymogu wdrożenia SMS na organizacje, wobec których Załącznik 19 nie ma zastosowania, może nie przynieść znaczących korzyści w zakresie bezpieczeństwa.

1.2.2 Rozszerzenie uznaniowego zastosowania SMS

1.2.2.1 Wymienione powyżej kryteria zastosowania mogą również służyć jako wytyczne dla Państw przy rozpatrywaniu rozszerzenia zastosowania SMS poza zakres określony w Załączniku 19 lub przy promowaniu dobrowolnego wdrożenia. Wprowadzenie uznaniowego zastosowania SMS powinno być dokładnie przemyślane. Decyzja o rozszerzeniu zastosowania SMS na sektory lub podmioty powinna uwzględniać ryzyka bezpieczeństwa zidentyfikowane przez Państwo, a jeżeli decyzja taka została podjęta, wdrożenie SMS powinno być monitorowane w ramach krajowego programu bezpieczeństwa. Przed wprowadzeniem wymogu wdrożenia SMS, Państwa proszone są o rozważenie, czy:

- a) istnieją inne realne możliwości osiągnięcia pożądaney poprawy w zakresie bezpieczeństwa; oraz
- b) Państwo i branża lotnicza dysponują wystarczającymi zasobami do wdrożenia i monitorowania SMS. W szczególności należy zwrócić uwagę na możliwy wpływ na personel oraz na ewentualne wyzwanie polegające na pozyskaniu i zintegrowaniu niezbędnych umiejętności i wiedzy.

1.2.2.2 Każde Państwo powinno rozważyć akceptowalny poziom bezpieczeństwa (ALoSP) w swojej branży i ustanowić schemat zastosowania SMS, który najbardziej prawdopodobnie pozwoli osiągnąć cele bezpieczeństwa Państwa. Wprowadzony schemat zastosowania SMS będzie prawdopodobnie ewoluował w kierunku ciągłego dostosowania do akceptowalnego poziomu bezpieczeństwa Państwa.

1.2.3 Odpowiedzialność za zarządzanie bezpieczeństwem

Żaden z przepisów zawartych w Załączniku 19 nie ma na celu przeniesienia na Państwo odpowiedzialności podmiotu lub operatora lotniczego. Państwa posiadają wiele narzędzi do zarządzania bezpieczeństwem przy pomocy swojego systemu. W ramach krajowego programu bezpieczeństwa każde Państwo powinno rozważyć najlepsze opcje nadzoru nad działalnością lotniczą lub nad nowymi formami działalności, które mogą nie być objęte zakresem obecnych Załączników ICAO.

1.2.4 Możliwość zastosowania przez podmioty państwowe lub wojskowe

1.2.4.1 W niektórych Państwach funkcję podmiotu lotniczego zapewnia strona cywilna lub wojskowa. Niektóre podmioty lotnicze świadczą usługi dla wojska na zlecenie, a niektóre organizacje wojskowe świadczą usługi cywilne. Niezależnie od ustaleń, podmiot lotniczy w danym Państwie powinien być zobowiązany do spełnienia wszystkich mających zastosowanie norm SARP ICAO, w tym wymagań SMS Załącznika 19, bez względu na szczególny charakter takiej organizacji. Opis systemu Państwa lub podmiotu lotniczego powinien uwzględniać funkcje tych organizacji i ich wzajemne relacje. Dyrektor odpowiedzialny podmiotu, zarówno cywilnego, jak i wojskowego, powinien być w stanie wyjaśnić ustalenia i sposób zarządzania ryzykami bezpieczeństwa. Mówiąc prościej, podmioty lotnicze powinny zarządzać bezpieczeństwem niezależnie od ustaleń organizacyjnych.

1.2.4.2 Jeżeli Państwo działa jako podmiot lotniczy, powinien istnieć wyraźny podział między jego funkcjami jako podmiotu i organu regulacyjnego. Osiąga się to poprzez jasne określenie ról i obowiązków organu danego Państwa i personelu podmiotu lotniczego w celu uniknięcia wszelkich konfliktów interesów.

1.2.5 Bezpieczeństwo i higiena pracy a bezpieczeństwo lotnicze

Bezpieczeństwo i higiena pracy (OSHE) to dziedzina zajmująca się bezpieczeństwem, zdrowiem i dobrobytem ludzi w pracy. Podstawową różnicą między zarządzaniem bezpieczeństwem lotniczym a systemami OSHE jest intencja. W wielu Państwach pracodawcy mają prawny obowiązek dbać o zdrowie i bezpieczeństwo swoich pracowników. Programy OSHE mają na celu spełnienie prawnych i etycznych obowiązków pracodawców poprzez wspieranie bezpiecznego i zdrowego środowiska pracy. Kwestie te są zazwyczaj rozpatrywane przez inny organ rządowy aniżeli ten, który zajmuje się sprawami lotniczymi. Zasadniczo, Załącznik 19, Rozdział 2, *Zastosowanie*, celowo koncentruje się na „funkcjach zarządzania bezpieczeństwem związanych z bezpieczną eksploatacją statków powietrznych lub funkcji stanowiących bezpośrednio jej wsparcie”.

1.3. WDROŻENIE ZARZĄDZANIA BEZPIECZEŃSTWEM

1.3.1 Ustanowienie solidnych podstaw ma istotne znaczenia dla skutecznego wdrożenia zarządzania bezpieczeństwem. Podczas wdrażania wymagań związanych z SSP lub SMS, w pierwszej kolejności należy uwzględnić następujące aspekty:

- a) *Zaangażowanie kierownictwa wyższego szczebla*: Zaangażowanie kierownictwa wyższego szczebla wszystkich państwowych instytucji lotniczych ma istotne znaczenie dla skutecznego wdrożenia zarządzania bezpieczeństwem.
- b) *Zgodność z wymaganiami normatywnymi*: Państwo powinno zapewnić skuteczny system nadzoru nad bezpieczeństwem w zakresie licencjonowania, certyfikacji, upoważniania i zatwierdzania osób fizycznych oraz organizacji lotniczych w swoim Państwie, w tym wykwalifikowanego personelu technicznego. Podmioty lotnicze powinny zapewnić, że wdrożyły procesy zapewniające stałą zgodność z ustanowionymi wymaganiami normatywnymi.
- c) *System egzekwowania*: Państwo powinno ustanowić politykę egzekwowania oraz ramy prawne umożliwiające stronom zarządzanie i rozstrzygnięcie odstępstw i drobnych naruszeń.
- d) *Ochrona informacji bezpieczeństwa*: Istotne jest, aby Państwa wprowadziły ochronne ramy prawne w celu zapewnienia stałej dostępności danych bezpieczeństwa oraz informacji bezpieczeństwa.

1.3.2 Opis systemu

Opis systemu to podsumowanie procesów, działań i interfejsów organizacji (Państwa lub podmiotu lotniczego), które muszą zostać ocenione pod kątem identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa, które są objęte jej systemem bezpieczeństwa. Przedstawia on system lotniczy, w którym funkcjonuje organizacja, oraz różne zaangażowane jednostki i organy. Opis odnosi się do interfejsów wewnątrz organizacji, a także do interfejsów z organizacjami zewnętrznymi, które przyczyniają się do bezpiecznego zapewniania usług. Opis systemu stanowi punkt wyjścia do wdrożenia SSP/SMS. Więcej informacji na temat opisu systemu Państw i podmiotów lotniczych znajduje się w Rozdziale 8 i 9, odpowiednio.

1.3.3 Interfejsy

1.3.3.1 Kiedy Państwa i podmioty lotnicze rozważają wdrożenie zarządzania bezpieczeństwem, ważne jest, aby uwzględnić ryzyka bezpieczeństwa spowodowane przez podmioty powiązane. Interfejsy mogą mieć charakter wewnętrzny (np. między operacjami a obsługą techniczną lub działem finansowym, HR lub prawnym) lub zewnętrzny (np. inne Państwo, podmiot lotniczy lub podwykonawca). Państwa i podmioty lotnicze mają większą kontrolę nad

wszelkimi powiązаныmi ryzykami bezpieczeństwa, kiedy interfejsy są zidentyfikowane i zarządzane. Interfejsy są definiowane jako część opisu systemu.

Ocena wpływu na bezpieczeństwo interfejsu

1.3.3.2 Kiedy Państwo lub podmiot lotniczy zidentyfikowały swoje interfejsy, ryzyko bezpieczeństwa stwarzane przez każdy interfejs jest oceniane przy użyciu istniejących w organizacji procesów oceny ryzyka bezpieczeństwa (patrz Rozdział 2 w celu uzyskania szczegółowych informacji). Na podstawie zidentyfikowanych ryzyk bezpieczeństwa, Państwo lub podmiot lotniczy mogą rozważyć współpracę z innymi organizacjami w celu określenia odpowiedniej strategii kontroli ryzyka bezpieczeństwa. Organizacje współpracujące mogą być w stanie zidentyfikować więcej zagrożeń ze strony interfejsów, dokonując oceny wszelkich powiązanych ryzyk bezpieczeństwa i określając wzajemnie odpowiednie środki kontroli. Współpraca jest w dużym stopniu pożądana, ponieważ postrzeganie ryzyka bezpieczeństwa może się różnić w zależności od organizacji.

1.3.3.3 Ważne jest również uznanie, że każda zaangażowana organizacja jest odpowiedzialna za identyfikację i zarządzanie wszelkimi zidentyfikowanymi zagrożeniami, które wpływają na organizację. Krytyczność interfejsu może być różna dla każdej organizacji. Każda organizacja może w sposób racjonalny stosować różne klasyfikacje ryzyka bezpieczeństwa oraz mieć różne priorytety ryzyka bezpieczeństwa (w kategoriach poziomu bezpieczeństwa, zasobów, czasu).

Monitorowanie i zarządzanie interfejsami

1.3.3.4 Państwa i podmioty lotnicze są odpowiedzialne za bieżące monitorowanie i zarządzanie swoimi interfejsami w celu zapewnienia bezpiecznego świadczenia usług. Skutecznym podejściem do zarządzania ryzykiem bezpieczeństwa interfejsów jest ustanowienie formalnych umów pomiędzy współdziałającymi organizacjami z jasno określonymi obowiązkami w zakresie monitorowania i zarządzania. Dokumentowanie i udostępnianie wszystkich problemów związanych z bezpieczeństwem interfejsów, zgłoszeń zdarzeń dotyczących bezpieczeństwa i zdobytych doświadczeń, a także ryzyk bezpieczeństwa pomiędzy współdziałającymi organizacjami, zapewni jasny obraz sytuacji. Udostępnianie umożliwi transfer wiedzy i praktyk roboczych, które mogłyby poprawić skuteczność w zakresie bezpieczeństwa każdej organizacji.

1.3.4 Planowanie wdrożenia

1.3.4.1 Przeprowadzenie analizy luk przed rozpoczęciem wdrażania SSP/SMS pozwoli organizacji na identyfikację luki między obecnymi strukturami organizacyjnymi i procesami, a tymi, które są wymagane do skutecznego działania SSP lub SMS. W przypadku SSP ważne jest uwzględnienie przeglądu list kontrolnych USOAP uznawanych za podstawę SSP.

1.3.4.2 Jak sama nazwa wskazuje, plan wdrożenia SSP lub SMS to plan mający na celu wdrożenie SSP/SMS. Zawiera on opis wymaganych zasobów, zadań i procesów, a także orientacyjny harmonogram czasowy i kolejność realizacji kluczowych zadań i obowiązków. Więcej informacji na temat wdrażania zarządzania bezpieczeństwem dla Państw i podmiotów prowadzących działalność w lotnictwie cywilnym znajdują się w Rozdziale 8 i 9, odpowiednio.

Ocena dojrzałości

1.3.4.3 Wkrótce po wdrożeniu kluczowych komponentów i elementów SSP lub SMS, należy przeprowadzać okresowe oceny w celu monitorowania skuteczności działania. W miarę dojrzewania systemu, organizacja powinna dążyć do zapewnienia, że działa on zgodnie z przeznaczeniem i jest skuteczny w osiągnięciu określonych celów bezpieczeństwa. Dojrzewanie zarządzania bezpieczeństwem wymaga czasu, a celem powinno być utrzymanie lub ciągłe podnoszenie poziomu bezpieczeństwa organizacji.

1.3.5 Kwestie związane z wielkością i złożonością

1.3.5.1 Każde Państwo i każdy podmiot lotniczy jest inny. Krajowe programy bezpieczeństwa (SSP) i systemy zarządzania bezpieczeństwem (SMS) są zaprojektowane w taki sposób, aby były dostosowane do specyficznych potrzeb każdego Państwa lub podmiotu. Wszystkie komponenty i wszystkie elementy SSP/SMS są ze sobą połączone i współzależne i są one niezbędne do skutecznego działania. Ważne jest, aby wymagania związane z SSP i SMS nie były wdrażane tylko w sposób nakazowy. Tradycyjne wymagania normatywne należy uzupełnić o podejście oparte na wydajności.

1.3.5.2 Program/system ma na celu zapewnienie pożądaných wyników dla każdej organizacji bez nadmiernego obciążenia. SSP i SMS, jeżeli zostały dobrze wdrożone, mają uzupełniać i ulepszać istniejące w organizacji systemy i procesy. Skuteczne zarządzanie bezpieczeństwem zostanie osiągnięte dzięki przemyślanemu planowaniu i wdrożeniu, gwarantując że każde wymaganie jest uwzględniane w sposób zgodny z kulturą i środowiskiem operacyjnym organizacji. Więcej informacji na temat czynników wymagających uwzględnienia podczas wdrażania SSP/SMS dla Państw i podmiotów lotniczych znajduje się w Rozdziale 8 i 9, odpowiednio.

1.3.6 Integracja podstawowych elementów

Należy zauważyć, że wszystkie systemy składają się z trzech podstawowych elementów: ludzi, procesów i technologii. Zarządzanie bezpieczeństwem nie jest wyjątkiem. Przy ustanawianiu lub utrzymywaniu różnych procesów, działań i funkcji, wszystkie Państwa i podmioty lotnicze powinny upewnić się, że uwzględniły intencję każdego wymogu i, co najważniejsze, w jaki sposób będą współpracować, aby umożliwić organizacji realizację jej celów bezpieczeństwa. Każdy z tych elementów zarządzania bezpieczeństwem oraz wzajemne powiązania zostaną omówione w niniejszym podręczniku.

1.4. ZINTEGROWANE ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA

1.4.1 System lotniczy jako całość obejmuje wiele różnych systemów funkcjonalnych, takich jak finanse, środowisko, bezpieczeństwo i ochrona. Dwa ostatnie elementy stanowią podstawowe dziedziny operacyjne większego systemu lotniczego. Jako koncepcje współdzielą one ważne cechy, ponieważ wszystkie związane są z ryzykiem zdarzeń z różnego stopnia następstwami. Niemniej jednak różnią się one istotnym elementem jakim jest intencja. Ochrona dotyczy złośliwych, celowych działań, które zakłócają działanie systemu. Bezpieczeństwo koncentruje się na negatywnym wpływie na działanie danych systemów, który spowodowany jest niezamierzonymi następstwami wielu czynników.

1.4.2 W kontekście operacyjnym, wszystkie systemy funkcjonalne powodują pewnego rodzaju ryzyko, które musi być właściwie zarządzane w celu zmniejszenia wszelkich niekorzystnych konsekwencji. Tradycyjnie każdy system wypracował specyficzne dla danego sektora zasady zarządzania ryzykiem i praktyki mające na celu uwzględnienie różnych cech każdego systemu. Większość tych praktyk dotyczących zarządzania ryzykiem obejmuje kompleksową analizę konsekwencji wewnątrzsystemowych, często określaną jako zarządzanie niezamierzonymi konsekwencjami. Innym aspektem są konsekwencje międzysystemowe wynikające z procesów zarządzania ryzykiem specyficznych dla systemu. Wynika to z faktu, że skuteczna strategia zarządzania ryzykiem jednego specyficznego sektora może mieć negatywny wpływ na inny operacyjny sektor lotnictwa. W lotnictwie najczęściej podkreślaną zależnością międzysystemową jest dylemat bezpieczeństwa/ochrona. Skuteczne środki ochrony mogą mieć negatywny wpływ na bezpieczeństwo i odwrotnie. Dziedziny bezpieczeństwa i ochrony mogą się różnić pod względem podstawowej intencji, ale zbiegają się we wspólny cel, jakim jest ochrona ludzi i mienia (np. zwalczanie zagrożeń cybernetycznych i ryzyk wymaga koordynacji w dziedzinie bezpieczeństwa i ochrony lotnictwa). W niektórych przypadkach zarządzanie nieodłącznym ryzykiem może wpłynąć na inną dziedzinę w nieprzewidywany sposób, na przykład:

- a) wzmocnione drzwi kokpitu wymagane ze względu na ryzyka dotyczące ochrony może mieć wpływ na eksploatację statku powietrznego;
- b) ograniczenia dotyczące przewozu osobistych urządzeń elektronicznych w kabynie mogą powodować przemieszczenie ryzyka dotyczącego ochrony z kabiny do ładowni, co prowadzi do zwiększonego ryzyka bezpieczeństwa; oraz
- c) zmiana tras w celu uniknięcia przelotów nad strefami konfliktu może skutkować załoczonymi korytarzami powietrznymi, które stanowią problem związany z bezpieczeństwem.

1.4.3 Skuteczne zarządzanie ryzykiem w lotnictwie powinno mieć na celu całościowe zmniejszenie ryzyka w systemie, w tym we wszystkich zaangażowanych systemach funkcjonalnych. Proces ten wymaga analitycznej oceny całego systemu na najwyższym poziomie odpowiedniej jednostki (Państwo, organizacje regionalne, podmioty prowadzące działalność w lotnictwie cywilnym). Ocena i integracja potrzeb systemu funkcjonalnego oraz współzależności są określane jako zintegrowane zarządzanie ryzykiem (IRM). IRM skupia się na całościowym zmniejszeniu ryzyka organizacji. Jest to osiągnięte poprzez ilościową i jakościową analizę zarówno ryzyka nieodłącznego, jak również skuteczności i wpływu procesów zarządzania ryzykiem specyficznym dla danego sektora. IRM skupia się na ogólnosystemowej koordynacji, harmonizacji i optymalizacji procesów zarządzania ryzykiem dla uzyskania jednego celu jakim jest zmniejszenie ryzyka. IRM nie może zastępować zarządzania ryzykiem operacyjnym systemów funkcjonalnych i nie ma na celu przekazywania im dodatkowych zadań i obowiązków. IRM stanowi odrębną koncepcję wysokiego szczebla, która wykorzystuje porady ekspertów w zakresie zarządzania ryzykiem specyficznym dla danego sektora i zapewnia całościowe informacje zwrotne w celu osiągnięcia najwyższego poziomu wydajności systemu na społecznie akceptowalnym poziomie. Więcej informacji na temat zarządzania ryzykiem bezpieczeństwa, które wchodzi w zakres niniejszego podręcznika, znajduje się w Rozdziale 2 i 8 (dla Państw) oraz w Rozdziale 9 (dla podmiotów prowadzących działalność w lotnictwie cywilnym).

Uwaga. – Struktura i zakresy odpowiedzialności w ramach rządu w danym Państwie mogą wpływać na nadzór nad każdym obszarem, na przykład, władze lotnictwa cywilnego (CAA) odpowiedzialne są za bezpieczeństwo lotnicze, podczas gdy agencja ochrony środowiska ponosi odpowiedzialność za nadzór nad środowiskiem. Każda instytucja prowadząca nadzór może mieć inne wymagania i metodologie.

ROZDZIAŁ 2

PODSTAWY ZARZĄDZANIA BEZPIECZEŃSTWEM

2.1. KONCEPCJA BEZPIECZEŃSTWA I JEGO EWOLUCJA

2.1.1 Niniejszy rozdział zawiera przegląd podstawowych koncepcji i praktyk związanych z zarządzaniem bezpieczeństwem. Ważne jest, aby zrozumieć te podstawy przed skupieniem się na specyficznych aspektach zarządzania bezpieczeństwem przedstawionych w kolejnych rozdziałach.

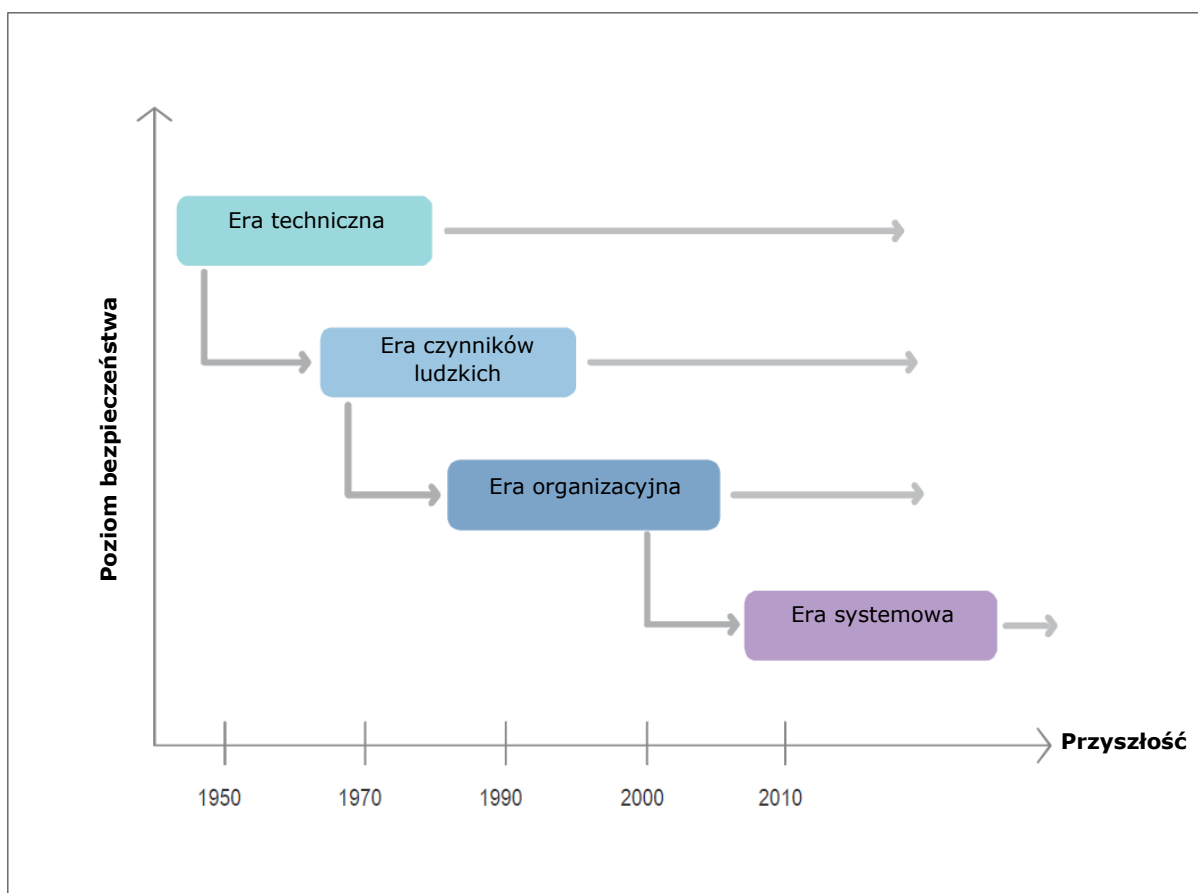
2.1.2 W kontekście lotnictwa, bezpieczeństwo jest „stanem, w którym ryzyka związane z działalnością lotniczą, dotyczące eksploatacji statków powietrznych lub bezpośrednio ją wspierające, są zmniejszone i kontrolowane do akceptowalnego poziomu”.

2.1.3 Bezpieczeństwo lotnicze ma charakter dynamiczny. Nowe zagrożenia i ryzyka bezpieczeństwa nieustannie się pojawiają i muszą być łagodzone. Dopóki ryzyka bezpieczeństwa są utrzymywane na odpowiednim poziomie kontroli, system tak otwarty i dynamiczny jak lotnictwo może być nadal bezpieczny. Należy zauważyć, że na akceptowalny poziom bezpieczeństwa mają często wpływ krajowe i międzynarodowe normy oraz czynniki kulturowe.

2.1.4 Postęp w zakresie bezpieczeństwa lotniczego można opisać za pomocą czterech podejść, które w przybliżeniu pokrywają się z erami działalności. Podejścia zostały wymienione poniżej i przedstawione na Rysunku 2-1.

- a) *Podejście techniczne* – Od początku XX wieku do końca lat sześćdziesiątych, lotnictwo stało się środkiem transportu masowego, w którym zidentyfikowane niedostatki w zakresie bezpieczeństwa były początkowo związane z czynnikami technicznymi i wadami technologicznymi. Przedsięwzięcia z zakresu bezpieczeństwa skupiały się na badaniu i poprawie czynników technicznych (na przykład statku powietrznego). Do lat 50-tych, postęp technologiczny doprowadził do stopniowego spadku częstotliwości wypadków, a procesy w zakresie bezpieczeństwa zostały poszerzone o zgodność z przepisami oraz nadzór.
- b) *Podejście z uwzględnieniem czynników ludzkich* – Na początku lat siedemdziesiątych, częstotliwość wypadków lotniczych znacznie spadła ze względu na duży postęp technologiczny i poprawę przepisów bezpieczeństwa. Lotnictwo stało się bezpieczniejszym środkiem transportu, a przedsięwzięcia z zakresu bezpieczeństwa poszerzone zostały o czynniki ludzkie, w tym takie jak „interfejs człowiek – maszyna”. Pomimo inwestowania zasobów w łagodzenie błędów, czynniki ludzkie nadal są wymieniane jako powtarzalny czynnik w wypadkach. Czynniki ludzkie skupiały się na jednostce, bez pełnego uwzględnienia kontekstu operacyjnego i organizacyjnego. Dopiero na początku lat dziewięćdziesiątych uznano, że jednostki działają w złożonym środowisku zawierającym wiele czynników, które mogą wpływać na zachowanie.
- c) *Podejście organizacyjne* – W połowie lat dziewięćdziesiątych bezpieczeństwo zaczęto postrzegać z perspektywy systemowej oraz zaczęto włączać czynniki organizacyjne jak również czynniki ludzkie i techniczne. Wprowadzono pojęcie „wypadku organizacyjnego”. Perspektywa ta uwzględniała wpływ takich kwestii jak kultura organizacyjna oraz polityka w zakresie skuteczności kontroli ryzyka bezpieczeństwa. Ponadto rutynowe gromadzenie i analiza danych bezpieczeństwa przy użyciu reaktywnych i proaktywnych metod umożliwiły organizacjom monitorowanie znanych ryzyk bezpieczeństwa i wykrywanie pojawiających się trendów w zakresie bezpieczeństwa. Te ulepszenia zapewniły wiedzę i podstawy, które doprowadziły do obecnego podejścia do zarządzania bezpieczeństwem.

- d) *Kompleksowe podejście systemowe* – Od początku XXI wieku wiele Państw i podmiotów lotniczych przyjęło podejścia do bezpieczeństwa z przeszłości i rozwinęło je do wyższego poziomu dojrzałości w zakresie bezpieczeństwa. Rozpoczęły one wdrażanie SSP lub SMS czerpiąc korzyści z bezpieczeństwa. Jednak dotychczasowe systemy bezpieczeństwa koncentrowały się głównie na indywidualnym poziomie bezpieczeństwa i kontroli lokalnej, przy minimalnym uwzględnieniu całego systemu lotniczego w szerszym kontekście. Doprowadziło to do rosnącego zrozumienia złożoności systemu lotniczego i różnych organizacji, które odgrywają istotną rolę w bezpieczeństwie lotniczym. Istnieje wiele przykładów wypadków i incydentów pokazujących, że interfejsy między organizacjami przyczyniły się do negatywnych wyników.



Rysunek 2-1. Ewolucja bezpieczeństwa

2.1.5 Stała ewolucja bezpieczeństwa doprowadziła Państwa i podmioty lotnicze do punktu, w którym istotnym elementem rozważań są interakcje i interfejsy pomiędzy elementami systemu: ludźmi, procesami i technologiami. Doprowadziło to do większego zrozumienia pozytywnej roli, jaką w systemie odgrywają ludzie. Bezpieczeństwo korzysta na współpracy pomiędzy podmiotami prowadzącymi działalność w lotnictwie cywilnym oraz pomiędzy podmiotami a Państwami. Ta perspektywa przyczyniła się do powstania wielu inicjatyw współpracy pomiędzy podmiotami lotniczymi i do docenienia korzyści płynących ze współpracy przy rozwiązywaniu problemów związanych z bezpieczeństwem. Dobrym tego przykładem jest Program ICAO ds. bezpieczeństwa na drodze startowej.

2.1.6 W celu dalszego rozwoju kompleksowego podejścia systemowego, interfejsy i interakcje pomiędzy organizacjami (w tym Państwami) muszą być dobrze zrozumiane i zarządzane. Państwa również zaczynają dostrzegać rolę, jaką kompleksowe podejście systemowe może odgrywać w rozwoju SSP. Na przykład, pomagają ono zarządzać ryzykami bezpieczeństwa, które występują w wielu działaniach lotniczych.

2.2. LUDZIE W SYSTEMIE

2.2.1 Sposób, w jaki ludzie postrzegają swoje obowiązki związane z bezpieczeństwem oraz sposób, w jaki współdziałają z innymi w celu wykonywania swoich zadań w miejscu pracy, znacząco wpływa na poziom bezpieczeństwa ich organizacji. Zarządzanie bezpieczeństwem musi uwzględniać sposób, w jaki ludzie przyczyniają się, zarówno pozytywnie, jak i negatywnie, do bezpieczeństwa organizacji. Czynniki ludzkie dotyczą zrozumienia sposobów wchodzenia przez ludzi w interakcję ze światem, ich możliwości i ograniczeń oraz wpływu na działania człowieka w celu poprawy w realizacji swoich zadań w pracy. W rezultacie, uwzględnienie czynników ludzkich stanowi integralną część zarządzania bezpieczeństwem, które jest konieczne, aby zrozumieć, zidentyfikować i zminimalizować ryzyka, a także zoptymalizować wkład człowieka w bezpieczeństwo organizacji.

2.2.2 Poniżej przedstawiono kluczowe sposoby, w jakie procesy zarządzania bezpieczeństwem uwzględniają czynniki ludzkie:

- a) zaangażowanie kierownictwa wyższego szczebla w tworzenie środowiska pracy optymalizującego działania człowieka i zachęcającego personel do aktywnego angażowania się w procesy zarządzania bezpieczeństwem organizacji;
- b) jednoznaczne określenie obowiązków personelu w zakresie zarządzania bezpieczeństwem w celu zapewnienia powszechnego zrozumienia i oczekiwań;
- c) zapewnienie personelowi informacji od organizacji, które:
 - 1) opisują oczekiwane zachowania w odniesieniu do procesów i procedur organizacji;
 - 2) opisują działania, jakie zostaną podjęte przez organizację w odpowiedzi na indywidualne zachowania;
- d) poziomy zasobów ludzkich są monitorowane i dostosowywane w taki sposób, aby zapewnić wystarczającą liczbę osób do zaspokojenia potrzeb operacyjnych;
- e) ustanowiono polityki, procesy i procedury w celu zachęcenia do zgłaszania zdarzeń dotyczących bezpieczeństwa;
- f) dane bezpieczeństwa i informacje bezpieczeństwa są analizowane, aby umożliwić uwzględnienie ryzyk związanych ze zmiennymi działaniami oraz ograniczenia człowieka, ze szczególnym uwzględnieniem wszelkich powiązanych czynników organizacyjnych i operacyjnych;
- g) opracowano polityki, procesy i procedury, które są jasne, zwarte i wykonalne, w celu:

- 1) optymalizacji działań człowieka;
 - 2) zapobiegania nieumyślnym błędom;
 - 3) zmniejszenia niepożądanych konsekwencji zmiennych działań człowieka; ich skuteczność jest stale monitorowana podczas normalnej pracy;
- a) bieżące monitorowanie normalnych operacji obejmuje ocenę, czy procesy i procedury są przestrzegane, a w przypadku gdy nie są one przestrzegane, prowadzone są dochodzenia w celu ustalenia przyczyny;
 - b) dochodzenia dotyczące bezpieczeństwa obejmują ocenę czynników ludzkich, w tym sprawdzenie nie tylko zachowań, ale również ich powodów (kontekst), przy założeniu, że w większości przypadków ludzie starają się wykonywać swoje zadania jak najlepiej potrafią;
 - c) proces zarządzania zmianami obejmuje uwzględnienie zmieniających się zadań i ról człowieka w systemie;
 - d) personel został przeszkolony w celu zapewnienia, że posiada on kompetencje do wykonywania swoich obowiązków, skuteczność szkolenia jest weryfikowana, a programy szkolenia dostosowywane do zmieniających się potrzeb.

2.2.3 Skuteczność zarządzania bezpieczeństwem zależy w dużej mierze od stopnia wsparcia i zaangażowania kierownictwa wyższego szczebla w tworzenie środowiska pracy, które optymalizuje działania człowieka i zachęca personel do aktywnego angażowania się i udziału w procesach zarządzania bezpieczeństwem organizacji.

2.2.4 Aby odnieść się do sposobu, w jaki organizacja wpływa na działania człowieka, musi istnieć wsparcie na wyższym szczeblu do wdrożenia skutecznego zarządzania bezpieczeństwem. Dotyczy to zobowiązania kierownictwa do stworzenia właściwego środowiska pracy i właściwej kultury bezpieczeństwa w celu uwzględnienia czynników ludzkich. Ma to również wpływ na postawy i zachowania wszystkich osób w organizacji. Więcej informacji na temat kultury bezpieczeństwa znajduje się w Rozdziale 3.

2.2.5 Stworzono szereg modeli wspierających ocenę wpływu czynników ludzkich na poziom bezpieczeństwa. Model SHELL jest powszechnie znany i przydatny do zilustrowania wpływu i interakcji różnych komponentów systemu na człowieka, oraz podkreśla potrzebę uwzględnienia czynników ludzkich jako integralnej części zarządzania ryzykiem bezpieczeństwa (SRM).

2.2.6 Rysunek 2-2 przedstawia związek pomiędzy ludźmi (w centrum modelu) a komponentami związanymi z miejscem pracy. Model SHELL zawiera cztery następujące komponenty:

- a) Oprogramowanie (S) [ang. *Software*]: procedury, szkolenia, wsparcie itp.;
- b) Sprzęt (H) [ang. *Hardware*]: maszyny i wyposażenie;
- c) Środowisko (E) [ang. *Environment*]: środowisko pracy, w którym reszta systemu L-H-S musi funkcjonować; oraz
- d) Człowiek (L) [ang. *Liveware*]: inni ludzie w miejscu pracy.



Rysunek 2-2. Model SHELL

2.2.7 *Człowiek*. Kluczowym elementem modelu są ludzie bezpośrednio zaangażowani w działania i przedstawieni w centrum modelu. Jednak ze wszystkich elementów wchodzących w skład modelu, jest to ten, który jest najmniej przewidywalny i najbardziej podatny na wpływy wewnętrzne (głód, zmęczenie, motywacja, itp.) oraz wpływy zewnętrzne (temperatura, światło, hałas, itp.). Choć ludzie posiadają niezwykłą zdolność adaptacji, podlegają znacznym różnicom w działaniu. Ludzie nie są wystandaryzowani w takim samym stopniu jak sprzęt, więc nie może być mowy o krawędziach bloku, które są proste i wyrównane. W celu uniknięcia napięć, które mogą zagrozić działaniom człowieka, należy rozumieć wpływ nieprawidłowości w interfejsach pomiędzy poszczególnymi blokami modelu SHELL a blokiem centralnym jakim jest człowiek. Nierówne krawędzie modułów stanowią odzwierciedlenie niedoskonałych połączeń każdego modułu. Jest to przydatne w wizualizacji poniższych interfejsów pomiędzy różnymi komponentami systemu lotniczego:

- a) *Człowiek-Sprzęt (L-H)*. Interfejs L-H odnosi się do relacji pomiędzy człowiekiem a fizycznymi cechami wyposażenia, maszyn i urządzeń. Uwzględnia ergonomię obsługi wyposażenia przez personel, sposób wyświetlania informacji dotyczących bezpieczeństwa oraz sposób oznakowania i obsługi przełączników i dźwigni, dzięki czemu są one logiczne i intuicyjne w obsłudze.
- b) *Człowiek-Oprogramowanie (L-S)*. Interfejs L-S to relacja pomiędzy człowiekiem a systemami wspomagającymi w miejscu pracy, np. przepisami, podręcznikami, listami kontrolnymi, publikacjami, procesami i procedurami oraz oprogramowaniem komputerowym. Obejmuje takie kwestie jak aktualność doświadczeń, dokładność, format i sposób prezentacji, słownictwo, czytelność i zastosowanie symboli. L-S uwzględnia procesy i procedury – czy są łatwe w realizacji i zrozumieniu.
- c) *Człowiek-Człowiek (L-L)*. Interfejs L-L to relacja i interakcja pomiędzy ludźmi w obrębie ich środowiska pracy. Niektóre z tych interakcji mają miejsce wewnątrz organizacji (koledzy, przełożeni, menedżerowie), wiele z nich ma miejsce pomiędzy poszczególnymi osobami z różnych organizacji, gdzie sprawują różne funkcje (kontrolerzy ruchu lotniczego z pilotami, piloci z inżynierami, itp.).

Interfejs L-L uwzględnia znaczenie komunikacji i umiejętności interpersonalnych, a także dynamikę grupy, w określaniu działań człowieka. Pojawienie się zarządzania zasobami załogi (CRM) i jego rozszerzenie na służby ruchu lotniczego (ATS) i obsługę techniczną umożliwiło organizacjom uwzględnienie działań zespołowych w zarządzaniu błędami. W zakres tego interfejsu wchodzi także relacje pomiędzy personelem a kierownictwem oraz kultura organizacyjna.

- d) *Człowiek–Środowisko (L-E)*. Ten interfejs obejmuje relację pomiędzy człowiekiem a środowiskiem. Dotyczy on takich kwestii jak temperatura, światło otoczenia, hałas, wibracje i jakość powietrza. Uwzględnia również zewnętrzne czynniki środowiskowe, takie jak pogoda, infrastruktura i teren.

2.3. ZWIĄZKI PRZYCZYNOWE WYPADKU

2.3.1 Model „sera szwajcarskiego” (lub Model Reasona), opracowany przez profesora Jamesa Reasona, i dobrze znany branży lotniczej, pokazuje, że wypadki związane są z kolejnymi naruszeniami wielu zabezpieczeń systemu. Naruszenia te mogą być aktywowane przez szereg czynników wspomagających, takich jak awarie sprzętu lub błędy operacyjne. Model sera szwajcarskiego zakłada, że złożone systemy, takie jak lotnictwo, są szczególnie dobrze chronione przez poziomy zabezpieczeń (inaczej zwane „barierami”). Jednostkowa awaria rzadko ma poważne konsekwencje. Naruszenie zabezpieczeń może być opóźnioną konsekwencją decyzji podejmowanych na wyższych szczeblach organizacji, które mogą pozostawać uśpione do czasu, kiedy ich skutki lub szkodliwy potencjał uaktywni się w wyniku określonych warunków operacyjnych (znanych jako stany ukryte). W takich szczególnych okolicznościach, uchybienia człowieka (lub „uchybienia aktywne”) na poziomie operacyjnym przyczyniają się do naruszenia ostatecznych poziomów zabezpieczeń. Model Reasona zakłada, że wszystkie wypadki stanowią połączenie zarówno uchybień aktywnych, jak i stanów ukrytych.

2.3.2 Uchybienia aktywne (ang. *active failures*) to działania lub zaniechania, w tym błędy i łamanie reguł, które mają natychmiastowy skutek negatywny. Z perspektywy czasu, są one postrzegane jako działania niebezpieczne. Uchybienia aktywne dotyczą personelu na pierwszej linii (piloci, kontrolerzy ruchu lotniczego, inżynierowie obsługi technicznej statku powietrznego, itp.) i mogą prowadzić do szkodliwych następstw.

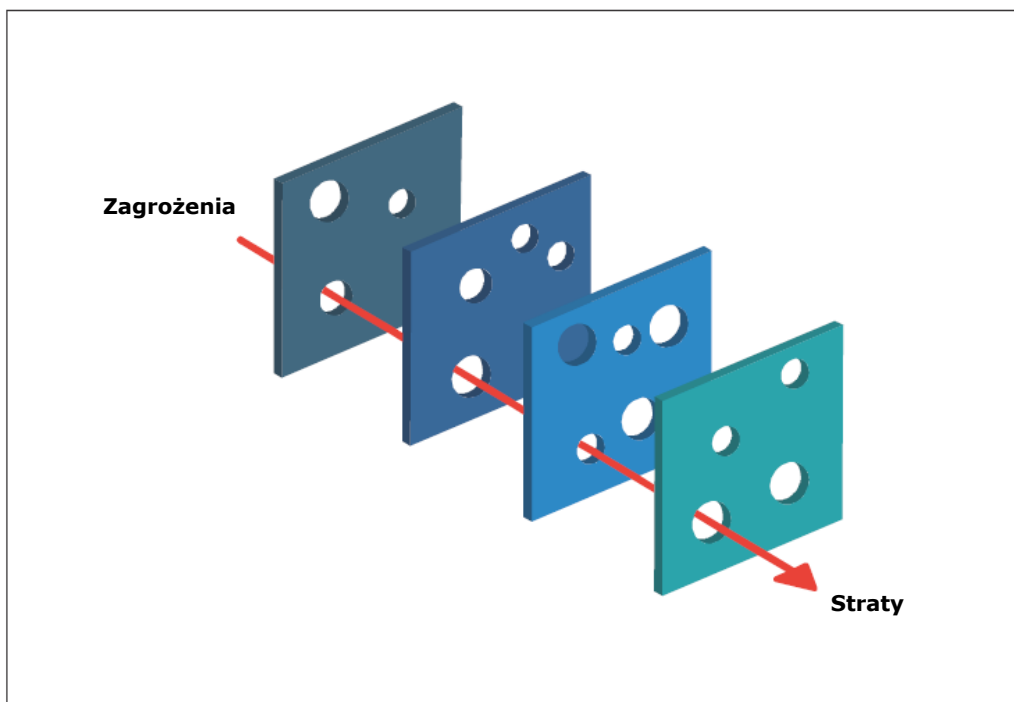
2.3.3 Stany ukryte (ang. *latent conditions*) mogą istnieć w systemie na długo przed pojawieniem się szkodliwych następstw. Konsekwencje stanów ukrytych mogą pozostawać uśpione przez długi czas. Początkowo, stany ukryte nie są postrzegane jako szkodliwe, ale w pewnych warunkach mogą stać się widoczne, gdy zostaną naruszone zabezpieczenia poziomu operacyjnego. Stany takie mogą zostać stworzone przez ludzi znajdujących się daleko od miejsca zdarzenia sensie czasowym i przestrzennym. Stany ukryte w systemie mogą obejmować stany wynikające z kultury bezpieczeństwa związane z wyborem sprzętu lub konstrukcją procedur, sprzecznymi celami organizacyjnymi, wadliwymi systemami organizacyjnymi lub decyzjami kierownictwa.

2.3.4 Pojęcie „wypadku z przyczyn organizacyjnych” pomaga zidentyfikować stany ukryte na podstawie działań ogólnosystemowych, a nie starań lokalnych, w celu ograniczenia do minimum uchybień aktywnych ze strony poszczególnych osób. Co ważne, stany ukryte, w momencie kiedy były tworzone, miały dobre intencje. Decydenci w organizacji często równoważą ograniczone zasoby i potencjalnie sprzeczne priorytety oraz koszty. Decyzje podejmowane codziennie w dużych organizacjach, w szczególnych okolicznościach, mogą nieumyślnie doprowadzić do szkodliwych następstw.

2.3.5 Rysunek 2-3 pokazuje, w jaki sposób model sera szwajcarskiego pomaga w zrozumieniu wzajemnego oddziaływania czynników organizacyjnych i zarządczych w związkach przyczynowych wypadku. System lotnictwa posiada wiele wbudowanych zabezpieczeń w celu ochrony przed zmiennością działań lub decyzji człowieka na wszystkich poziomach organizacji. Niemniej jednak każda warstwa ma zazwyczaj słabe punkty, co zostało przedstawione w postaci otworów w plastrach „sera szwajcarskiego”. Czasami wszystkie słabe punkty ustawiają się w tej samej linii (przedstawione w postaci wyrównanych otworów) prowadząc do naruszenia, które przenika wszystkie bariery obronne i może skutkować katastrofalnymi następstwami. Model sera szwajcarskiego

przedstawia sposób, w jaki stany ukryte są zawsze obecne w systemie i w jaki mogą się objawiać w wyniku lokalnych czynników uruchamiających.

2.3.6 Istotne jest, aby zdawać sobie sprawę, że na niektóre zabezpieczenia lub naruszenia mogą mieć wpływ organizacje współpracujące. Dlatego niezwykle ważne jest, aby podmioty lotnicze oceniały i zarządzały tymi interfejsami.



Rysunek 2-3. Konceptcja związków przyczynowych wypadku

2.3.7 Zastosowanie modelu „sera szwajcarskiego” w zarządzaniu bezpieczeństwem

2.3.7.1 Model „sera szwajcarskiego” może być używany jako przewodnik analityczny zarówno przez Państwa, jak i podmioty lotnicze poprzez przyjrzenie się osobom zaangażowanym w incydent lub zidentyfikowane zagrożenie, w okoliczności organizacyjne, które mogły pozwolić na zaistnienie sytuacji. Może on być stosowany podczas zarządzania ryzykiem bezpieczeństwa, nadzoru nad bezpieczeństwem, audytu wewnętrznego, zarządzania zmianami i badaniami bezpieczeństwa. W każdym przypadku model można wykorzystać do rozważenia, które zabezpieczenia organizacji są skuteczne, które mogły być lub zostały naruszone, oraz w jakich miejscach system może skorzystać z dodatkowych zabezpieczeń. Po zidentyfikowaniu, wszelkie słabe elementy zabezpieczeń mogą zostać wzmocnione przed wypadkami i incydentami, które mogą mieć miejsce w przyszłości.

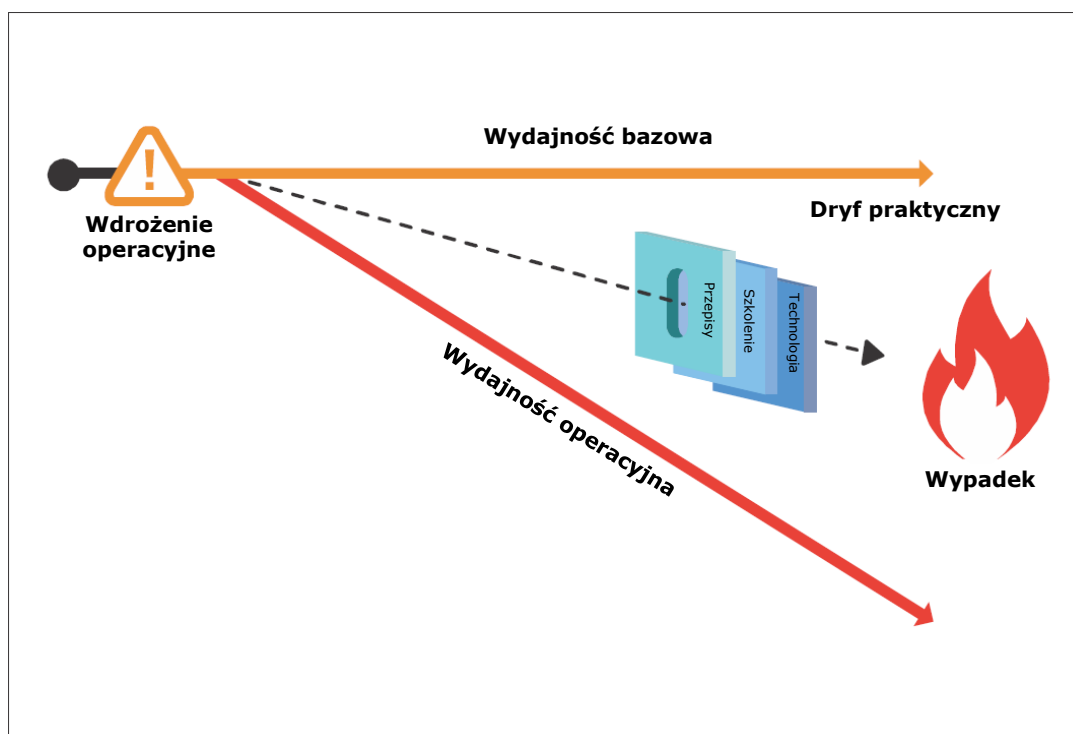
2.3.7.2 W praktyce, zdarzenie naruszy zabezpieczenia zgodnie z kierunkiem strzałki (zagrożenie → straty), jak przedstawiono na Rysunku 2-3. Oceny sytuacji będą prowadzone w przeciwnym kierunku, w tym przypadku od strat do zagrożenia. Rzeczywiste wypadki lotnicze zazwyczaj zawierają pewien stopień złożoności. Istnieją bardziej zaawansowane modele, które mogą pomóc Państwom i podmiotom lotniczym zrozumieć, w jaki sposób i dlaczego wypadki się zdarzają.

2.3.8 Dryf praktyczny

2.3.8.1 Teoria dryfu praktycznego Scotta A. Snooka jest wykorzystywana do zrozumienia, w jaki sposób działanie dowolnego systemu oddala się od jego pierwotnego projektu. Zadania, procedury i sprzęt są często początkowo projektowane i planowane w środowisku teoretycznym, w idealnych warunkach, z ukrytym założeniem, że prawie wszystko można przewidzieć i kontrolować, i że wszystko działa zgodnie z oczekiwaniami. Zwykle opiera się to na trzech podstawowych założeniach:

- a) technologia potrzebna do osiągnięcia celów produkcyjnych systemu jest dostępna;
- b) personel jest przeszkolony, kompetentny i zmotywowany do prawidłowej obsługi technologii zgodnie z przeznaczeniem; oraz
- c) polityka i procedury będą dyktować zachowanie systemu i człowieka.

Te założenia leżą u podstaw bazowej (lub idealnej) wydajności systemu, którą można przedstawić graficznie jako linię prostą od momentu wdrożenia operacyjnego, jak przedstawiono na Rysunku 2-4.



Rysunek 2-4. Koncepcja dryfu praktycznego

2.3.8.2 Po wdrożeniu operacyjnym, system powinien działać idealnie w sposób, w jaki został zaprojektowany, zgodnie z wydajnością bazową (pomarańczowa linia) przez większość czasu. W rzeczywistości wydajność operacyjna często różni się od zakładanej wydajności bazowej w wyniku rzeczywistych operacji, które prowadzone są w złożonym, ciągle zmieniającym się i zazwyczaj wymagającym środowisku (czerwona linia). Ponieważ dryf jest konsekwencją codziennej praktyki, określa się go mianem „dryfu praktycznego”. Termin „dryf” jest w tym kontekście używany jako stopniowe odchodzenie od zamierzonego kursu z powodu wpływów zewnętrznych.

2.3.8.3 Snook kwestionuje fakt, że dryf praktyczny jest nieunikniony w każdym systemie, bez względu na to, jak ostrożny i przemyślany jest jego projekt. Niektóre powody dryfu praktycznego to:

- a) technologia, która nie działa zgodnie z przewidywaniami;
- b) procedury, których nie można wykonać zgodnie z planem w określonych warunkach operacyjnych;
- c) zmiany w systemie, w tym dodatkowe komponenty;
- d) interakcje z innymi systemami;
- e) kultura bezpieczeństwa;
- f) odpowiedniość (lub nieodpowiedniość) zasobów (np. sprzętu pomocniczego);
- g) uczenie się na sukcesach i porażkach w celu usprawnienia operacji, itp.

2.3.8.4 W rzeczywistości ludzie zazwyczaj sprawiają, że system będzie działał codziennie, pomimo niedociągnięć systemu, poprzez zastosowanie lokalnych modyfikacji (lub obejść) i strategii osobistych. Te obejścia mogą polegać na pominięciu ochrony zapewnianej przez istniejące środki kontrolne i obronne przed ryzykiem bezpieczeństwa.

2.3.8.5 Działania związane z zapewnianiem bezpieczeństwa, takie jak audyty, obserwacje i monitorowanie wskaźników poziomu bezpieczeństwa, mogą pomóc w ujawnieniu działań, które ulegają zjawisku dryfu praktycznego. Analiza informacji dotyczących bezpieczeństwa mająca na celu uzyskanie informacji dlaczego dryf ma miejsce, pomaga w łagodzeniu ryzyk bezpieczeństwa. Im bliżej początku wdrożenia operacyjnego kiedy dryf praktyczny jest identyfikowany, tym łatwiej organizacji podjąć interwencję. Więcej informacji na temat zapewnienia bezpieczeństwa dla Państw i podmiotów prowadzących działalność w lotnictwie cywilnym znajduje się w Rozdziale 8 i 9, odpowiednio.

2.4. DYLEMAT ZARZĄDZANIA

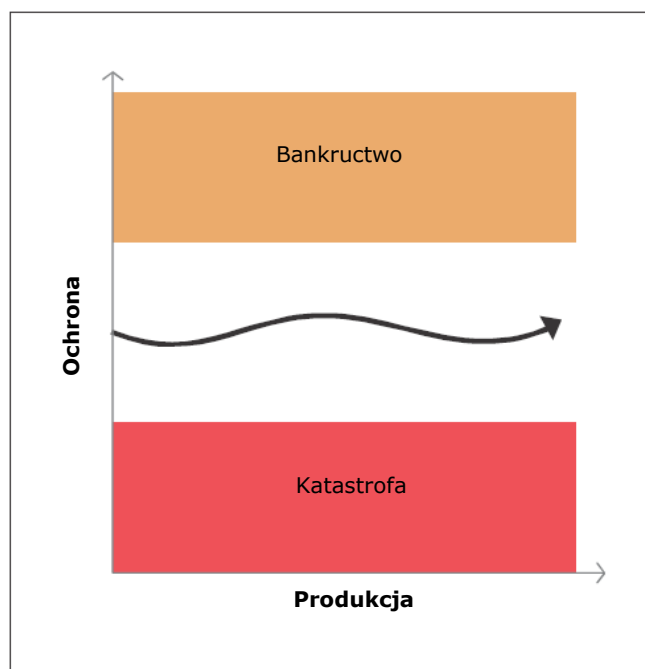
2.4.1 W każdej organizacji zaangażowanej w świadczenie usług, produkcja/rentowność oraz ryzyka bezpieczeństwa są ze sobą powiązane. Organizacja musi utrzymać rentowność, aby utrzymać działalność, równoważąc produkcję z akceptowalnymi ryzykami bezpieczeństwa (i kosztami związanymi z wdrażaniem środków kontroli ryzyka bezpieczeństwa). Typowe środki kontroli ryzyka bezpieczeństwa obejmują technologię, szkolenie, procesy i procedury. W przypadku Państwa, środki te są podobne, tj. szkolenie personelu, odpowiednie wykorzystanie technologii, skuteczny nadzór oraz wewnętrzne procesy i procedury wspierające nadzór. Wdrożenie środków kontroli ryzyka bezpieczeństwa ma swoją cenę – środki finansowe, czas, zasoby – a ich celem jest zazwyczaj poprawa bezpieczeństwa, a nie produkcji. Jednak niektóre inwestycje w „ochronę” mogą również poprawić „produkcję”, zmniejszając liczbę wypadków i incydentów, a tym samym związane z nimi koszty.

2.4.2 Przestrzeń bezpieczeństwa stanowi metaforę odnoszącą się do strefy, w której organizacja równoważy pożądaną produkcję/rentowność przy zachowaniu wymaganej ochrony bezpieczeństwa poprzez środki kontroli ryzyka bezpieczeństwa. Na przykład, podmiot prowadzący działalność może chcieć zainwestować w nowy sprzęt. Nowy sprzęt może jednocześnie zapewnić niezbędną poprawę wydajności, a także poprawić niezawodność i poziom bezpieczeństwa. Takie podejmowanie decyzji wiąże się z oceną zarówno korzyści dla organizacji, jak i związanych z tym ryzyk bezpieczeństwa. Przydział nadmiernych środków na mechanizmy kontroli ryzyka bezpieczeństwa może spowodować, że działalność stanie się nieopłacalna, co zagrazi rentowności organizacji.

2.4.3 Z drugiej strony, przydział nadmiernych środków na produkcję kosztem ochrony może mieć wpływ na produkt lub usługę, co może ostatecznie doprowadzić do wypadku. Istotne jest zatem, aby zdefiniować granicę bezpieczeństwa, która zapewnia wczesne ostrzeżenie o istnieniu, bądź rozwoju, niezrównoważonego przydziału środków. Organizacje wykorzystują systemy zarządzania finansami w celu rozpoznawania sytuacji, w których zbliżają się do granicy bankructwa i stosują tę samą logikę i narzędzia wykorzystywane w ramach zarządzania

bezpieczeństwem do monitorowania poziomu bezpieczeństwa. Dzięki temu organizacja może działać rentownie i bezpiecznie w obrębie przestrzeni bezpieczeństwa. Rysunek 2-5 ilustruje granice przestrzeni bezpieczeństwa organizacji. Organizacje muszą stale monitorować i zarządzać swoją przestrzenią bezpieczeństwa, ponieważ ryzyka bezpieczeństwa i wpływy zewnętrzne z upływem czasu ulegają zmianie.

2.4.4 Potrzeba zrównoważenia rentowności i bezpieczeństwa (lub produkcji i ochrony) stała się szybko zrozumianym i zaakceptowanym wymogiem z perspektywy podmiotu prowadzącego działalność. Równowaga ta ma również zastosowanie do zarządzania bezpieczeństwem przez Państwo, biorąc pod uwagę wymóg zrównoważenia zasobów wymaganych do pełnienia przez Państwo funkcji ochronnych, które obejmują certyfikację i nadzór.



Rysunek 2-5. Koncepcja przestrzeni bezpieczeństwa

2.5. ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA

Zarządzanie ryzykiem bezpieczeństwa (SRM) stanowi kluczowy element zarządzania bezpieczeństwem i obejmuje identyfikację zagrożeń, ocenę ryzyka bezpieczeństwa, łagodzenie ryzyka bezpieczeństwa oraz akceptację ryzyka. SRM to działanie ciągłe, ponieważ system lotniczy stale się zmienia, pojawiają się nowe zagrożenia, a niektóre zagrożenia i związane z nimi ryzyka bezpieczeństwa mogą się zmieniać z upływem czasu. Ponadto skuteczność wdrożonych strategii łagodzenia ryzyka bezpieczeństwa musi być monitorowana w celu określenia, czy konieczne są dalsze działania.

2.5.1 Wprowadzenie do zagrożeń

2.5.1.1 W lotnictwie zagrożenie można uznać za uśpiony potencjał szkód, który jest obecny w takiej czy innej formie w systemie lub w jego otoczeniu. Ten potencjał szkód może występować w różnych formach, na przykład: jako stan naturalny (np. teren) lub stan techniczny (np. oznakowanie poziome drogi startowej).

2.5.1.2 Zagrożenia są nieodłączną częścią działalności lotniczej, jednak ich występowanie i możliwe niekorzystne konsekwencje mogą być rozwiązane za pomocą strategii łagodzenia, które mają na celu ograniczenie potencjalnego zagrożenia skutkującego stanem niebezpiecznym. Lotnictwo może współistnieć z zagrożeniami, o ile są one kontrolowane. Identyfikacja zagrożeń stanowi pierwszy krok w procesie zarządzania ryzykiem bezpieczeństwa (SRM). Poprzedza ona ocenę ryzyka bezpieczeństwa i wymaga jasnego zrozumienia zagrożeń i związanych z nimi konsekwencji.

2.5.2 Zrozumienie zagrożeń i ich konsekwencji

2.5.2.1 Identyfikacja zagrożeń koncentruje się na warunkach lub obiektach, które mogą spowodować lub przyczynić się do niebezpiecznej eksploatacji statku powietrznego lub sprzętu, produktów i usług związanych z bezpieczeństwem lotniczym (wytyczne dotyczące odróżniania zagrożeń bezpośrednio związanych z bezpieczeństwem lotniczym od innych ogólnych/branżowych zagrożeń zostały omówione w kolejnych punktach).

2.5.2.2 Rozważmy, na przykład, sytuację kiedy występuje wiatr o prędkości piętnastu węzłów. Wiatr o prędkości piętnastu węzłów niekoniecznie oznacza stan niebezpieczny. W rzeczywistości taki wiatr wiejący bezpośrednio w dół drogi startowej poprawia osiągi statku powietrznego podczas startu i lądowania. Ale jeżeli wiatr o prędkości piętnastu wieje w poprzek drogi startowej, powstaje wiatr boczny, który może być niebezpieczny dla wykonywanej operacji. Wynika to z jego potencjału spowodowania niestabilności statku powietrznego. Zmniejszenie sterowania może doprowadzić do zdarzenia, takiego jak wypadnięcie z drogi startowej.

2.5.2.3 Powszechnym zjawiskiem jest mylenie zagrożeń z ich konsekwencjami. Konsekwencja to wynik, który może zostać wywołany przez zagrożenie. Na przykład, wypadnięcie z drogi startowej (wyjechanie poza drogę startową) jest potencjalną konsekwencją związaną z zagrożeniem jakim jest zanieczyszczona droga startowa. Poprzez jasne zdefiniowanie zagrożenia w pierwszej kolejności, łatwiej jest zidentyfikować możliwe konsekwencje.

2.5.2.4 W powyższym przykładzie dotyczącym wiatru bocznego, natychmiastowym skutkiem zagrożenia może być utrata sterowności bocznej, po której następuje wypadnięcie z drogi startowej. Ostateczną konsekwencją może być wypadek. Szkodliwy potencjał zagrożenia może się zmaterializować w postaci jednej lub wielu konsekwencji. Ważne jest, aby oceny ryzyka bezpieczeństwa identyfikowały wszystkie możliwe konsekwencje. Najbardziej skrajna konsekwencja – utrata życia ludzkiego – powinna być odróżniona od mniejszych konsekwencji, takich jak incydenty lotnicze; zwiększone obciążenie pracą załogi lotniczej lub dyskomfort pasażera. Opis konsekwencji będzie zawierał ocenę ryzyka, a następnie opracowanie i wdrożenie środków łagodzących poprzez ustalenie priorytetów i przydział środków. Szczegółowa i dokładna identyfikacja zagrożeń spowoduje dokładniejszą ocenę ryzyka bezpieczeństwa

Identyfikacja zagrożeń i ustalanie priorytetów

2.5.2.5 Zagrożenia występują na wszystkich poziomach organizacji i są wykrywalne za pomocą wielu źródeł, w tym systemów zgłaszania, inspekcji, audytów, burzy mózgów i oceny ekspertów. Mają one na celu proaktywne identyfikowanie zagrożeń, zanim doprowadzą one do wypadków, incydentów lub innych zdarzeń związanych z bezpieczeństwem. Ważnym mechanizmem proaktywnej identyfikacji zagrożeń jest dobrowolny system zgłaszania zdarzeń dotyczących bezpieczeństwa. Dodatkowe wytyczne dotyczące dobrowolnych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa znajdują się w Rozdziale 5. Informacje zebrane za pośrednictwem takich systemów zgłaszania można uzupełnić obserwacjami lub ustaleniami odnotowanymi podczas rutynowych inspekcji na miejscu lub audytów organizacji.

2.5.2.6 Zagrożenia można również zidentyfikować podczas przeglądu lub studium raportów z wewnętrznych i zewnętrznych badań. Uwzględnienie zagrożeń podczas przeglądu raportów z badań wypadków lub incydentów jest dobrym sposobem na poprawę systemu identyfikacji zagrożeń w organizacji. Jest to szczególnie ważne w sytuacji, gdy kultura bezpieczeństwa organizacji nie jest jeszcze wystarczająco dojrzała, aby mogła wspierać skuteczne dobrowolne zgłaszanie zdarzeń dotyczących bezpieczeństwa, lub w małych organizacjach o ograniczonej liczbie zdarzeń lub zgłoszeń. Ważnym źródłem konkretnych zagrożeń związanych z operacjami i działaniami są źródła zewnętrzne, takie jak ICAO, stowarzyszenia branżowe lub inne organy międzynarodowe.

2.5.2.7 Identyfikacja zagrożeń może również uwzględniać zagrożenia generowane poza organizacją jak również zagrożenia, które są poza bezpośrednią kontrolą organizacji, takie jak ekstremalne warunki pogodowe lub popiół wulkaniczny. Zagrożenia związane z pojawiającymi się ryzykami bezpieczeństwa stanowią również istotny środek w przygotowaniu się przez organizację na sytuacje, które mogą ostatecznie wystąpić.

2.5.2.8 Podczas identyfikacji zagrożeń należy wziąć pod uwagę następujące kwestie:

- a) opis systemu;
- b) czynniki projektowe, w tym projektowanie sprzętu i zadań;
- c) ograniczenia człowieka (np. fizjologiczne, psychologiczne, fizyczne i poznawcze);
- d) procedury i praktyki operacyjne, w tym dokumentacja i listy kontrolne oraz ich walidacja w rzeczywistych warunkach pracy;
- e) czynniki związane z komunikacją, w tym media, terminologia i język;

- f) czynniki organizacyjne, np. związane z rekrutacją, szkoleniem i zatrzymaniem personelu, zgodność celów produkcji i bezpieczeństwa, przydział środków, presja operacyjna i korporacyjna kultura bezpieczeństwa;
- g) czynniki związane ze środowiskiem operacyjnym (np. pogoda, hałas otoczenia i wibracje, temperatura i oświetlenie);
- h) czynniki związane z nadzorem w zakresie przepisów, w tym zastosowanie i wykonalność przepisów oraz certyfikacja sprzętu, personelu i procedur;
- i) systemy monitorowania działań, które mogą wykryć dryf praktyczny, odchylenia operacyjne lub pogorszenie wiarygodności produktu;
- j) czynniki związane z interfejsem człowiek-maszyna; oraz
- k) czynniki związane z interfejsami SSP/SMS z innymi organizacjami.

Zagrożenia związane z bezpieczeństwem i higieną pracy

2.5.2.9 Ryzyka bezpieczeństwa związane ze złożonymi zagrożeniami, które jednocześnie wpływają na bezpieczeństwo lotnicze jak również na bezpieczeństwo i higienę pracy, mogą być zarządzane poprzez oddzielne (równoległe) procesy łagodzenia ryzyka w celu uwzględnienia oddzielnych konsekwencji dla lotnictwa i BHP. Alternatywnie, można zastosować zintegrowany system łagodzenia ryzyka w lotnictwie i w zakresie BHP w celu uwzględnienia zagrożeń złożonych. Przykładem zagrożenia złożonego jest uderzenie pioruna w statek powietrzny na lotnisku. Inspektor BHP może uznać to zagrożenie za „zagrożenie w miejscu pracy” (personel naziemny/bezpieczeństwo w miejscu pracy). Dla inspektora bezpieczeństwa lotniczego jest to również zagrożenie lotnicze z ryzykiem uszkodzenia statku powietrznego i ryzykiem dla bezpieczeństwa pasażerów. Ważne jest, aby wziąć pod uwagę zarówno konsekwencje związane z BHP, jak i z bezpieczeństwem lotniczym przy tak złożonym zagrożeniu, ponieważ nie zawsze są one takie same. Cel i ukierunkowanie kontroli prewencyjnych w przypadku konsekwencji związanych z BHP i bezpieczeństwem lotniczym mogą się różnić.

Metodologie identyfikacji zagrożeń

2.5.2.10 Dwie główne metodologie identyfikacji zagrożeń to:

- a) *Reaktywna*. Metodologia ta obejmuje analizę wyników lub zdarzeń mających miejsce w przeszłości. Zagrożenia są identyfikowane poprzez badanie zdarzeń związanych z bezpieczeństwem. Incydenty i wypadki są wskazaniem niedociągnięć systemu i dlatego mogą być wykorzystane do określenia, które zagrożenie(a) przyczyniły się do zdarzenia.
- b) *Proaktywna*. Metodologia ta obejmuje zbieranie danych dotyczących bezpieczeństwa o zdarzeniach lub procesach o mniejszych konsekwencjach oraz analizę informacji dotyczących bezpieczeństwa lub częstotliwości występowania w celu określenia czy zagrożenie może prowadzić do wypadku lub incydentu. Informacje bezpieczeństwa dla proaktywnej identyfikacji zagrożeń pochodzą głównie z programów analizy danych o locie (FDA), systemów zgłaszania zdarzeń związanych z bezpieczeństwem oraz funkcji zapewniania bezpieczeństwa.

2.5.2.11 Zagrożenia można również identyfikować poprzez analizę danych bezpieczeństwa, która wskazuje niekorzystne trendy i przewiduje nowe zagrożenia, itp.

Zagrożenia związane z interfejsami SMS z organizacjami zewnętrznymi

2.5.2.12 Organizacje powinny również identyfikować zagrożenia związane z ich interfejsami zarządzania bezpieczeństwem. W miarę możliwości powinno to być realizowane jako wspólne przedsięwzięcie z organizacjami powiązаныmi. Identyfikacja zagrożeń powinna uwzględniać środowisko operacyjne i różne możliwości organizacyjne (ludzie, procesy, technologie), które mogą przyczynić się do bezpiecznego dostarczenia usługi lub dostępności, funkcjonalności lub wydajności produktu.

2.5.2.13 Przykładowo obsługa statku powietrznego angażuje wiele organizacji oraz personel operacyjny pracujący wewnątrz i na zewnątrz statku powietrznego. Prawdopodobnie pojawią się zagrożenia związane z interfejsami pomiędzy personelem operacyjnym, jego wyposażeniem a koordynacją działań w trakcie obsługi.

2.5.3 Prawdopodobieństwo ryzyka bezpieczeństwa

2.5.3.1 Prawdopodobieństwo ryzyka bezpieczeństwa to prawdopodobieństwo wystąpienia konsekwencji lub wyniku związanego z bezpieczeństwem. Ważne jest rozważenie różnych scenariuszy, tak aby można było uwzględnić wszystkie potencjalne konsekwencje. Poniższe pytania mogą pomóc w określeniu prawdopodobieństwa:

- a) Czy istnieje historia zdarzeń podobnych do rozważanego lub czy jest to odosobnione zdarzenie?
- b) Jaki inny sprzęt lub komponenty tego samego typu mogą mieć podobne problemy?
- c) Jaka jest liczba pracowników, którzy realizują lub podlegają określonym procedurom?
- d) Jaki jest zakres występowania rozważanego zagrożenia? Na przykład, jaki procent operacji wykorzystuje dany sprzęt lub działanie?

2.5.3.2 Uwzględnienie wszelkich czynników, które mogą stanowić podstawę tych pytań, pomoże w ocenie prawdopodobieństwa konsekwencji zagrożenia w każdym możliwym do przewidzenia scenariuszu.

2.5.3.3 Zdarzenie jest uważane za przewidywalne, jeżeli jakakolwiek rozsądna osoba mogłaby oczekiwać, że dany rodzaj zdarzenia będzie miał miejsce w tych samych okolicznościach. Identyfikacja każdego możliwego lub teoretycznie możliwego zagrożenia nie jest możliwa. Dlatego wymagana jest dobra ocena mająca na celu określenie odpowiedniego poziomu szczegółowości w identyfikacji zagrożeń. Podmioty prowadzące działalność w lotnictwie cywilnym powinny dołożyć należytej staranności przy identyfikacji znaczących i racjonalnie przewidywalnych zagrożeń związanych z ich produktem lub usługą.

Uwaga. – W odniesieniu do projektu produktu, termin „przewidywalny” ma być zgodny z jego zastosowaniem w przepisach, polityce i wytycznych dotyczących zdolności do lotu.

2.5.3.4 Tabela 1 przedstawia typową klasyfikację prawdopodobieństwa ryzyka bezpieczeństwa. Obejmuje ona pięć kategorii oznaczających prawdopodobieństwo związane z niebezpiecznym zdarzeniem lub stanem, opis każdej kategorii oraz przypisanie wartości do każdej z nich. W przykładzie tym zastosowano terminy jakościowe; można zdefiniować terminy ilościowe w celu zapewnienia dokładniejszej oceny. Będzie to zależało od dostępności odpowiednich danych dotyczących bezpieczeństwa oraz stopnia zaawansowania organizacji i operacji.

Tabela 1. Tabela prawdopodobieństwa ryzyka bezpieczeństwa

<i>Prawdopodobieństwo</i>	<i>Znaczenie</i>	<i>Wartość liczbowa</i>
Częste	Prawdopodobnie wystąpi wiele razy (występowało często)	5
Sporadyczne	Prawdopodobnie wystąpi od czasu do czasu (występowało niezbyt często)	4
Dalekie	Prawdopodobnie nie wystąpi, ale jest to możliwe (występowało rzadko)	3
Nieprawdopodobne	Bardzo mało prawdopodobne, że wystąpi (przypadek wystąpienia nie jest znany)	2
Skrajnie nieprawdopodobne	Prawie niewyobrażalne, że kiedykolwiek może wystąpić	1

Uwaga. – Powyższa tabela stanowi jedynie przykład. Poziom szczegółowości i złożoności tabel i macryc powinien być dostosowany do szczególnych potrzeb i złożoności każdej organizacji. Należy również zauważyć, że organizacje mogą uwzględnić zarówno kryteria jakościowe, jak i ilościowe.

2.5.4 Dotkliwość ryzyka bezpieczeństwa

2.5.4.1 Po zakończeniu oceny prawdopodobieństwa, następnym krokiem jest ocena dotkliwości, z uwzględnieniem potencjalnych konsekwencji związanych z zagrożeniem. Dotkliwość ryzyka bezpieczeństwa definiuje się jako zakres szkód, których można się spodziewać w konsekwencji lub wyniku zidentyfikowanego zagrożenia. Klasyfikacja dotkliwości powinna uwzględniać:

- a) ofiary śmiertelne lub poważne obrażenia, które wystąpiłyby w wyniku:

- 1) przebywania na pokładzie statku powietrznego;
 - 2) bezpośredniego kontaktu z dowolną częścią statku powietrznego, w tym części, które się odłączyły od statku powietrznego; lub
 - 3) bezpośredniego narażenia na podmuch z silników odrzutowych; oraz
- b) uszkodzenie:
- 1) uszkodzenie lub awaria konstrukcji statku powietrznego, które:
 - i) niekorzystnie wpływają na wytrzymałość konstrukcyjną, osiągi lub charakterystyki lotu statku powietrznego;
 - ii) normalnie wymagałyby poważnej naprawy lub wymiany danego elementu;
 - 2) uszkodzenie poniesione przez ATS lub urządzenia lotniskowe, które:
 - i) niekorzystnie wpływa na zarządzanie separacją statków powietrznych; lub
 - ii) niekorzystnie wpływa na zdolność lądowania.

2.5.4.2 Ocena dotkliwości powinna uwzględniać wszystkie możliwe konsekwencje związane z zagrożeniem, biorąc pod uwagę najgorszą przewidywalną sytuację. Tabela 2 przedstawia typową tabelę dotkliwości ryzyka bezpieczeństwa. Zawiera pięć kategorii oznaczających poziom dotkliwości, opis każdej kategorii i wartości przypisane do każdej kategorii. Podobnie jak w przypadku tabeli prawdopodobieństwa ryzyka bezpieczeństwa, tabela ta stanowi jedynie przykład.

Tabela 2. Przykładowa tabela dotkliwości ryzyka bezpieczeństwa

<i>Dotkliwość</i>	<i>Znaczenie</i>	<i>Wartość</i>
Katastrofalna	<ul style="list-style-type: none"> • Zniszczenie sprzętu/statku powietrznego • Wiele ofiar śmiertelnych 	A
Niebezpieczna	<ul style="list-style-type: none"> • Duża zmniejszenie marginesów bezpieczeństwa, fizyczne dolegliwości lub obciążenie personelu operacyjnego w takim stopniu, że nie ma pewności, że będzie wykonywał swoje zadania dokładnie lub w całości • Poważne obrażenia • Duże uszkodzenie sprzętu 	B
Większa	<ul style="list-style-type: none"> • Znaczne zmniejszenie marginesów bezpieczeństwa, zmniejszenie zdolności personelu operacyjnego do radzenia sobie z niekorzystnymi warunkami pracy w wyniku zwiększenia obciążenia pracą lub w wyniku pogorszenia warunków pracy • Poważny incydent • Obrażenia wśród ludzi 	C
Niewielka	<ul style="list-style-type: none"> • Uciążliwość • Ograniczenia operacyjne • Stosowanie procedur awaryjnych • Drobnny incydent 	D
Nieistotna	<ul style="list-style-type: none"> • Niewielkie konsekwencje 	E

2.5.5 Tolerancja ryzyka bezpieczeństwa

2.5.5.1 Indeks ryzyka bezpieczeństwa jest tworzony poprzez połączenie wyników prawdopodobieństwa i dotkliwości. W powyższym przykładzie, jest to oznaczenie alfanumeryczne. Odpowiednie kombinacje dotkliwości/prawdopodobieństwa zostały przedstawione w macyrycy oceny ryzyka bezpieczeństwa w Tabeli 3. Macyryca oceny ryzyka bezpieczeństwa jest stosowana do określenia tolerancji ryzyka bezpieczeństwa. Rozważmy, dla przykładu, sytuację, w której prawdopodobieństwo ryzyka bezpieczeństwa zostało ocenione jako sporadyczne (4), a dotkliwość ryzyka bezpieczeństwa została oceniona jako niebezpieczna (B), co skutkuje indeksem ryzyka bezpieczeństwa (4B).

Tabela 3. Przykładowa macyryca ryzyka bezpieczeństwa

<i>Ryzyko bezpieczeństwa</i>		<i>Dotkliwość</i>				
		<i>Katastrofalna</i> A	<i>Niebezpieczna</i> B	<i>Poważna</i> C	<i>Niewielka</i> D	<i>Nieistotna</i> E
<i>Prawdopodobieństwo</i>						
Częste	5	5A	5B	5C	5D	5E
Sporadyczne	4	4A	4B	4C	4D	4E
Odległe	3	3A	3B	3C	3D	3E
Nieprawdopodobne	2	2A	2B	2C	2D	2E
Skrajnie nieprawdopodobne	1	1A	1B	1C	1D	1E

Uwaga. – Przy określaniu tolerancji ryzyka bezpieczeństwa, należy wziąć pod uwagę jakość i wiarygodność danych wykorzystywanych do identyfikacji zagrożeń oraz prawdopodobieństwo ryzyka bezpieczeństwa.

2.5.5.2 Indeks uzyskany z macyrycy oceny ryzyka bezpieczeństwa powinien być następnie eksportowany do tabeli tolerancji ryzyka bezpieczeństwa, która opisuje - w formie narracyjnej - kryteria tolerancji dla danej organizacji. Tabela 4 przedstawia przykład tabeli tolerancji ryzyka bezpieczeństwa. Korzystając z powyższego przykładu, kryterium ryzyka bezpieczeństwa ocenionego jako 4B należy do kategorii „nie dopuszczalne”. W takim przypadku, indeks ryzyka bezpieczeństwa jest nieakceptowalny. Organizacja powinna zatem podjąć działania związane z kontrolą ryzyka, aby:

- zmniejszyć narażenie organizacji na określone ryzyko, tj. zmniejszyć komponent prawdopodobieństwa ryzyka do akceptowalnego poziomu;
- zmniejszyć dotkliwość konsekwencji związanych z zagrożeniem, tj. zmniejszyć komponent dotkliwości ryzyka do akceptowalnego poziomu; lub
- zmniejszyć zarówno dotkliwość, jak i prawdopodobieństwo, aby ryzyko było zarządzane do akceptowalnego poziomu.

2.5.5.3 Ryzyka bezpieczeństwa są pojęciowo oceniane jako akceptowalne, dopuszczalne lub niedopuszczalne. Ryzyka bezpieczeństwa oceniane początkowo jako niedopuszczalne są w żadnym wypadku nieakceptowalne. Prawdopodobieństwo i/lub dotkliwość konsekwencji zagrożeń są tak duże, a szkodliwy potencjał zagrożenia stwarza taką groźbę dla bezpieczeństwa, że wymagane jest działanie łagodzące lub wstrzymanie prowadzonych działań.

Tabela 4. Przykładowa tolerancja ryzyka bezpieczeństwa

<i>Zakres indeksu ryzyka bezpieczeństwa</i>	<i>Opis ryzyka bezpieczeństwa</i>	<i>Zalecane działania</i>
5A, 5B, 5C, 4A, 4B, 3A	NIEDOPUSZCZALNE	Należy podjąć natychmiastowe działania w celu łagodzenia ryzyka lub zaprzestania działań. Należy wykonać priorytetowe działania łagodzące ryzyko bezpieczeństwa w celu zapewnienia, że wdrożone zostały dodatkowe lub ulepszone prewencyjne środki kontrolne w celu obniżenia indeksu ryzyka bezpieczeństwa do ryzyka dopuszczalnego.
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A	DOPUSZCZALNE	Może być tolerowane w oparciu o działania łagodzące ryzyko bezpieczeństwa. Może być wymagana decyzja kierownictwa dotycząca akceptacji ryzyka.
3E, 2D, 2E, 1B, 1C, 1D, 1E	AKCEPTOWALNE	Akceptowalne w obecnej formie. Nie są wymagane żadne dalsze działania łagodzące ryzyko bezpieczeństwa.

2.5.6 Ocena ryzyk związanych z czynnikami ludzkimi

2.5.6.1 Uwzględnienie czynników ludzkich ma szczególne znaczenie w zarządzaniu ryzykiem bezpieczeństwa (SRM), ponieważ ludzie mogą być zarówno źródłem, jak i rozwiązaniem ryzyk bezpieczeństwa poprzez:

- a) przyczynianie się do wypadku lub incydentu poprzez zmienne działania wynikające z ograniczeń ludzkich;
- b) przewidywanie i podejmowanie odpowiednich działań w celu uniknięcia niebezpiecznej sytuacji: oraz
- c) rozwiązywanie problemów, podejmowanie decyzji oraz wykonywanie działań w celu łagodzenia ryzyk.

2.5.6.2 Dlatego ważne jest, aby w identyfikację, ocenę i łagodzenie ryzyka angażować ludzi posiadających odpowiednią wiedzę na temat czynników ludzkich.

2.5.6.3 SRM wymaga uwzględnienia wszystkich aspektów ryzyka bezpieczeństwa, w tym aspektów związanych z ludźmi. Ocena ryzyk związanych z działaniami człowieka jest bardziej złożona niż czynniki ryzyka związane z technologią i środowiskiem ponieważ:

- a) działania człowieka są bardzo zmienne, wykazują szeroki zakres oddziaływujących na siebie wpływów, wewnętrznych i zewnętrznych dla danej jednostki. Wiele spośród skutków oddziaływania pomiędzy tymi wpływami jest trudnych lub niemożliwych do przewidzenia; oraz
- b) konsekwencje zmiennych działań człowieka będą się różnić w zależności od wykonywanego zadania i kontekstu.

2.5.6.4 Powoduje to komplikacje w określaniu prawdopodobieństwa i dotkliwości ryzyka. Dlatego specjalistyczna wiedza w zakresie czynników ludzkich jest cenna w identyfikacji i ocenie ryzyk bezpieczeństwa. (Zarządzanie zmęczeniem za pomocą procesów SMS zostało opisane w *Podręczniku nadzoru nad podejściami do zarządzania zmęczeniem* (Doc 9966)).

2.5.7 Strategie łagodzenia ryzyka bezpieczeństwa

2.5.7.1 Łagodzenie ryzyka bezpieczeństwa jest często określane jako kontrola ryzyka bezpieczeństwa. Ryzyka bezpieczeństwa powinny być zarządzane do akceptowalnego poziomu poprzez łagodzenie ryzyka bezpieczeństwa poprzez zastosowanie odpowiednich środków kontroli ryzyka bezpieczeństwa. Należy to zrównoważyć z czasem, kosztem i trudnością podjęcia działań w celu zmniejszenia lub wyeliminowania ryzyka bezpieczeństwa. Poziom ryzyka bezpieczeństwa można obniżyć poprzez zmniejszenie dotkliwości potencjalnych konsekwencji, zmniejszenie prawdopodobieństwa wystąpienia lub zmniejszenie narażenia na to ryzyko bezpieczeństwa. Łatwiej i częściej można zmniejszyć prawdopodobieństwo, aniżeli zmniejszyć dotkliwość.

2.5.7.2 Łagodzenie ryzyka bezpieczeństwa to działania, które często skutkują zmianami w procedurach operacyjnych, wyposażeniu lub infrastrukturze. Strategie łagodzenia ryzyka bezpieczeństwa można podzielić na trzy kategorie:

- a) *Unikanie*: Operacja lub działanie jest odwoływane lub unikane, ponieważ ryzyko bezpieczeństwa przekracza korzyści wynikające z kontynuacji działania, eliminując w ten sposób ryzyko bezpieczeństwa całkowicie.
- b) *Zmniejszanie*: Częstotliwość operacji lub działania jest zmniejszana lub podejmowane jest działanie mające na celu zmniejszenie wielkości konsekwencji ryzyka bezpieczeństwa.
- c) *Segregacja*: Podejmowane jest działanie mające na celu odizolowanie skutków konsekwencji ryzyka bezpieczeństwa lub wbudowanie elementów nadmiarowości w celu ochrony przed nimi.

2.5.7.3 Uwzględnienie czynników ludzkich stanowi integralną część identyfikacji skutecznych działań łagodzących, ponieważ ludzie są zobowiązani do stosowania lub udziału w działaniach łagodzących lub naprawczych. Na przykład, działania łagodzące mogą obejmować wykorzystanie procesów lub procedur. Bez wkładu osób, które będą ich używać w rzeczywistych sytuacjach i/lub osób ze specjalistyczną wiedzą na temat czynników ludzkich, opracowane procesy lub procedury mogą nie spełniać swojego celu i powodować niezamierzone konsekwencje. Ponadto ograniczenia człowieka powinny być traktowane jako część każdego działania łagodzącego ryzyko bezpieczeństwa, budując strategie wychwytywania błędów w celu rozwiązania problemu zmiennych działań człowieka. W efekcie końcowym, ta ważna perspektywa czynnika ludzkiego skutkuje bardziej kompleksowymi i skutecznymi działaniami łagodzącymi.

2.5.7.4 Strategia łagodzenia ryzyka bezpieczeństwa może obejmować jedno z opisanych powyżej podejść lub może obejmować wiele podejść. Ważne jest, aby rozważyć pełen zakres możliwych środków kontrolnych w celu uzyskania rozwiązania optymalnego. Skuteczność każdej alternatywnej strategii musi zostać oceniona przed podjęciem decyzji. Każda proponowana alternatywna strategia łagodzenia ryzyka bezpieczeństwa powinna zostać zbadana z następujących perspektyw:

- a) *Skuteczność*. Zakres, w jakim działania alternatywne zmniejszają lub eliminują ryzyka bezpieczeństwa. Skuteczność można określić w kategoriach technicznych, szkoleniowych i prawnych zabezpieczeń, które mogą zmniejszyć lub wyeliminować ryzyka bezpieczeństwa.
- b) *Koszt/korzyść*. Zakres, w jakim przewidywane korzyści działania łagodzącego przewyższają koszty.
- c) *Praktyczność*. Zakres, w jakim działanie łagodzące można wdrożyć i w jakim jest właściwe pod względem dostępnej technologii, zasobów finansowych i administracyjnych, ustawodawstwa, woli politycznej, realiów operacyjnych, itp.
- d) *Akceptowalność*. Zakres, w jakim alternatywa jest akceptowalna dla osób, od których oczekuje się jej stosowania.

- e) *Wykonalność*. Zakres, w jakim można monitorować zgodność z nowymi zasadami, przepisami lub procedurami operacyjnymi.
- f) *Trwałość*. Zakres, w jakim działanie łagodzące będzie trwałe i skuteczne.
- g) *Pozostałe ryzyka bezpieczeństwa*. Stopień ryzyka bezpieczeństwa, który pozostaje po wdrożeniu wstępnego działania łagodzącego, i który może wymagać dodatkowych środków kontroli ryzyka bezpieczeństwa.
- h) *Niezamierzone konsekwencje*. Wprowadzenie nowych zagrożeń i związanych z nimi ryzyk bezpieczeństwa w wyniku wdrożenia jakiegokolwiek alternatywnego działania łagodzącego.
- i) *Czas*. Czas potrzebny na wdrożenia alternatywnego działania łagodzącego ryzyko bezpieczeństwa.

2.5.7.5 Działania naprawcze powinny uwzględniać wszelkie istniejące zabezpieczenia i ich (nie)zdolność do osiągnięcia akceptowalnego poziomu ryzyka bezpieczeństwa. Może to skutkować przeglądem wcześniejszych ocen ryzyka bezpieczeństwa, na które mogły mieć wpływ działania naprawcze. Działania łagodzące i kontrolne ryzyka bezpieczeństwa będą musiały zostać zweryfikowane/skontrolowane w celu zapewnienia, że są one skuteczne. Inny sposób monitorowania skuteczności działań łagodzących polega na wykorzystaniu wskaźników poziomu bezpieczeństwa (SPI). Więcej informacji na temat zarządzania bezpieczeństwem i SPI znajduje się w Rozdziale 4.

2.5.8 Dokumentacja zarządzania ryzykiem bezpieczeństwa

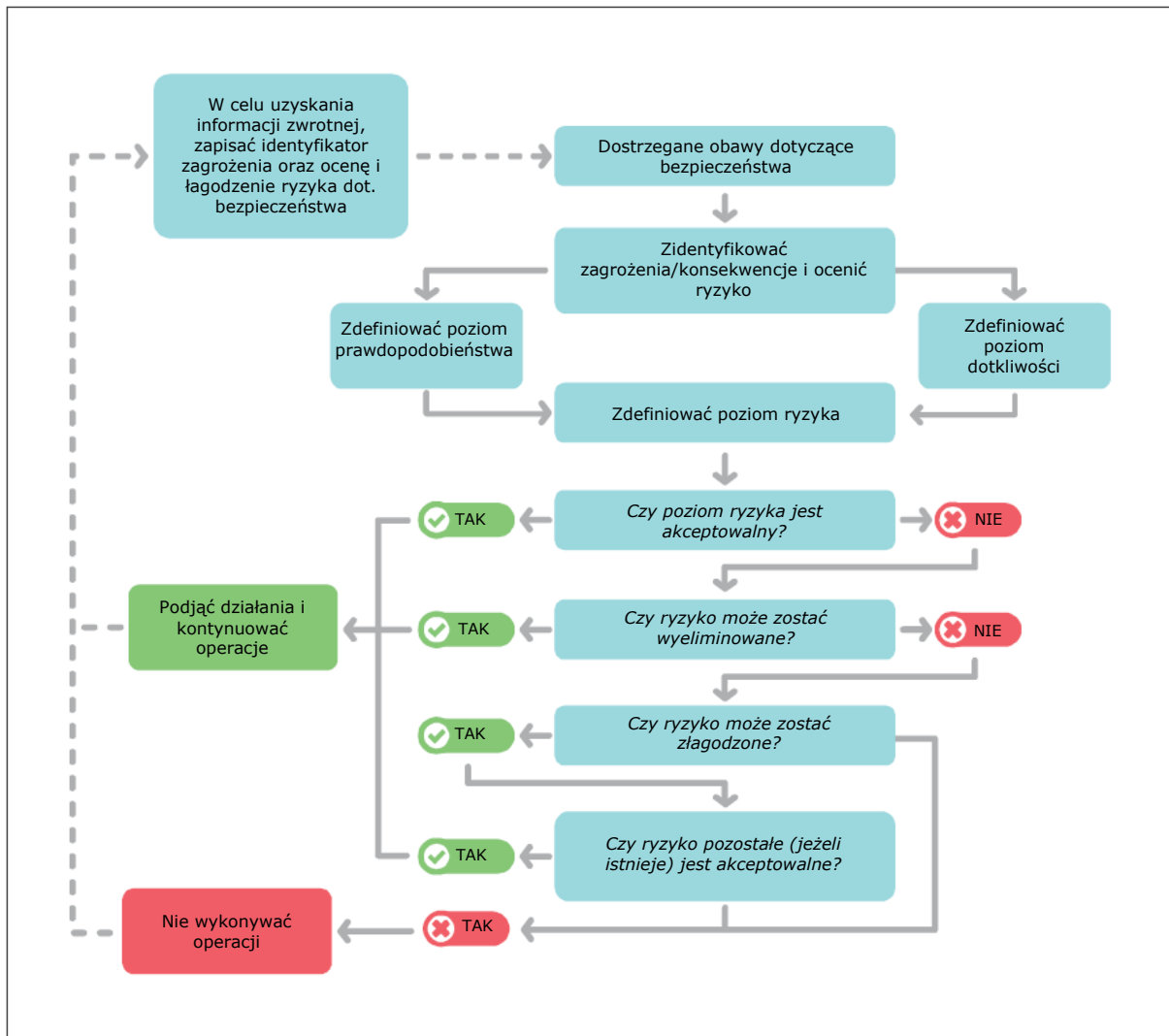
2.5.8.1 Działania związane z zarządzaniem ryzykiem bezpieczeństwa powinny być udokumentowane, obejmując wszelkie założenia leżące u podstaw oceny prawdopodobieństwa i dotkliwości, podjęte decyzje i wszelkie podjęte działania łagodzące ryzyko bezpieczeństwa. Można to zrobić za pomocą arkusza kalkulacyjnego lub tabeli. Niektóre organizacje mogą korzystać z bazy danych lub innego oprogramowania, w którym można przechowywać i analizować duże ilości danych bezpieczeństwa oraz informacji bezpieczeństwa.

2.5.8.2 Prowadzenie rejestru zidentyfikowanych zagrożeń ogranicza do minimum prawdopodobieństwo, że organizacja straci z pola widzenia swoje znane zagrożenia. W przypadku zidentyfikowania zagrożeń można je porównać ze znanymi zagrożeniami znajdującymi się w rejestrze, oraz sprawdzić, czy zagrożenie zostało już zarejestrowane i jakie działania zostały podjęte w celu jego łagodzenia. Rejestry zagrożeń mają zazwyczaj formę tabeli i zwykle obejmują: zagrożenie, potencjalne konsekwencje, ocenę powiązanych ryzyk, datę identyfikacji, kategorię zagrożenia, krótki opis, kiedy i gdzie ma zastosowanie, kto je zidentyfikował oraz jakie środki zostały wdrożone w celu łagodzenia ryzyk.

2.5.8.3 Narzędzia i procesy podejmowania decyzji związanych z ryzykiem bezpieczeństwa mogą być wykorzystane do poprawy powtarzalności i uzasadnienia decyzji w zakresie bezpieczeństwa podejmowanych przez decydentów organizacji. Przykład pomocy w podejmowaniu decyzji związanych z ryzykiem bezpieczeństwa został przedstawiony poniżej na Rysunku 2-6.

2.5.9 Analiza kosztów i korzyści

Analiza kosztów i korzyści lub efektywności kosztowej jest zwykle przeprowadzana podczas działań łagodzących ryzyko bezpieczeństwa. Jest to często związane z zarządzaniem przedsiębiorstwem, takim jak ocena skutków regulacji lub procesy zarządzania projektem. Mogą jednak wystąpić sytuacje, w których ocena ryzyka bezpieczeństwa może mieć znaczący wpływ na finanse. W takich sytuacjach uzasadnione może być wykonanie dodatkowej analizy kosztów i korzyści lub procesu opłacalności w celu wsparcia oceny ryzyka bezpieczeństwa. Zapewni to analizę opłacalności lub uzasadnienie zalecanych działań w zakresie kontroli ryzyka bezpieczeństwa, wraz z powiązanymi konsekwencjami finansowymi.



Rysunek 2-6. Pomoc w podejmowaniu decyzji związanych z zarządzaniem ryzykiem bezpieczeństwa

ROZDZIAŁ 3

KULTURA BEZPIECZEŃSTWA

3.1. WSTĘP

3.1.1 Kultura bezpieczeństwa jest naturalną konsekwencją posiadania ludzi w systemie lotniczym. Kultura bezpieczeństwa została opisana jako „sposób, w jaki ludzie zachowują się w odniesieniu do bezpieczeństwa i ryzyka, gdy nikt nie patrzy”. Jest wyrazem tego, w jaki sposób kierownictwo i pracownicy w organizacji postrzegają i cenią bezpieczeństwo, i jest odzwierciedlona poprzez zakres, w jakim osoby i grupy:

- a) są świadome ryzyk i znanych zagrożeń, na jakie narażona jest organizacja i prowadzona przez nią działalność;
- b) wykazują się ciągłymi zachowaniami mającymi na celu utrzymanie i zwiększenie bezpieczeństwa;
- c) mają dostęp do zasobów wymaganych do prowadzenia bezpiecznych operacji;
- d) mają chęć i zdolność do adaptacji w obliczu problemów związanych z bezpieczeństwem;
- e) mają chęć do komunikowania kwestii dotyczących bezpieczeństwa; oraz
- f) prowadzą konsekwentną ocenę zachowań związanych z bezpieczeństwem w całej organizacji.

3.1.2 Załącznik 19 wymaga, aby zarówno Państwa, jak i podmioty prowadzące działalność w lotnictwie cywilnym promowały pozytywną kulturę bezpieczeństwa w celu wspierania skutecznej realizacji zarządzania bezpieczeństwem poprzez SSP/SMS. Ten rozdział zawiera wytyczne na temat promocji pozytywnej kultury bezpieczeństwa.

3.2. KULTURA BEZPIECZEŃSTWA I ZARZĄDZANIE BEZPIECZEŃSTWEM

3.2.1 Niezależnie od tego, czy organizacja zdaje sobie z tego sprawę, czy też nie, będzie ona posiadać wiele różnych „kultur bezpieczeństwa”, które odzwierciedlają postawy i zachowania na poziomie grupy. Żadne dwie organizacje nie są identyczne, a nawet w obrębie tej samej organizacji, różne grupy mogą mieć różne sposoby myślenia o bezpieczeństwie, mówienia o bezpieczeństwie i działania w zakresie problemów związanych z bezpieczeństwem. To zróżnicowanie może być odpowiednie dla różnego rodzaju działań.

3.2.2 Sposób włączenia wartości dotyczących bezpieczeństwa do praktyk kierownictwa i personelu wpływa bezpośrednio na sposób ustanowienia i utrzymania kluczowych elementów krajowego programu bezpieczeństwa (SSP) i systemu zarządzania bezpieczeństwem (SMS). W konsekwencji, kultura bezpieczeństwa ma bezpośredni wpływ na poziom bezpieczeństwa. Jeżeli ktoś wierzy, że bezpieczeństwo nie jest tak ważne, obejścia, działania na skróty lub niebezpieczne decyzje lub osądy mogą być wynikiem takiego podejścia, zwłaszcza gdy ryzyko jest postrzegane jako niskie i brak jest widocznych konsekwencji lub niebezpieczeństwa. Kultura bezpieczeństwa organizacji ma zatem znaczący wpływ na rozwój i skuteczność SSP lub SMS. Kultura bezpieczeństwa to prawdopodobnie najważniejszy pojedynczy czynnik wpływający na zarządzanie bezpieczeństwem. Jeżeli organizacja ustanowiła wszystkie wymagania związane z zarządzaniem bezpieczeństwem, ale nie posiada pozytywnej kultury bezpieczeństwa, prawdopodobnie osiągnie gorsze wyniki.

3.2.3 Kiedy organizacja posiada pozytywną kulturę bezpieczeństwa, i jest ona wyraźnie wspierana przez kierownictwo wyższego i średniego szczebla, personel na pierwszej linii ma poczucie współodpowiedzialności za osiąganie celów bezpieczeństwa organizacji. Skuteczne zarządzanie bezpieczeństwem stanowi również wsparcie dla wysiłków zmierzających w kierunku coraz bardziej pozytywnej kultury bezpieczeństwa poprzez zwiększenie widoczności wsparcia kierownictwa i poprawę zaangażowania personelu w zarządzanie ryzykiem bezpieczeństwa.

3.2.4 Pozytywna kultura bezpieczeństwa opiera się na wysokim stopniu zaufania i szacunku pomiędzy personelem a kierownictwem. Potrzebny jest czas i wysiłek, aby zbudować pozytywną kulturę bezpieczeństwa, która może łatwo ulec uszkodzeniu w wyniku decyzji i działań lub zaniechań kierownictwa. Należy podejmować nieustanne wysiłki i działania wzmacniające. Kiedy przywództwo aktywnie popiera bezpieczne praktyki, stają się one normalnym sposobem działania. Idealną sytuacją jest w pełni wdrożony i skuteczny SSP/SMS oraz pozytywna kultura bezpieczeństwa. Dlatego kultura bezpieczeństwa organizacji jest często postrzegana jako odzwierciedlenie dojrzałości SSP/SMS. Skuteczne zarządzanie bezpieczeństwem umożliwia pozytywną kulturę bezpieczeństwa, a pozytywna kultura bezpieczeństwa umożliwia skuteczne zarządzanie bezpieczeństwem.

3.2.5 Kultura bezpieczeństwa i jej wpływ na zgłaszanie zdarzeń związanych z bezpieczeństwem

3.2.5.1 Krajowy program bezpieczeństwa i system zarządzania bezpieczeństwem korzystają z danych bezpieczeństwa i informacji bezpieczeństwa, które są niezbędne do rozwiązania istniejących i potencjalnych niedociągnięć w zakresie bezpieczeństwa oraz zagrożeń, w tym problemów związanych z bezpieczeństwem zidentyfikowanych przez personel. Sukces systemu zgłaszania zdarzeń związanych z bezpieczeństwem zależy wyłącznie od ciągłego przepływu informacji od organizacji i osób, a następnie informacji zwrotnych do nich. Ochrona danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł ma zasadnicze znaczenie dla zapewnienia ciągłej dostępności informacji. Na przykład, w dobrowolnych systemach zgłaszania można to osiągnąć za pomocą systemu, który jest poufny i nie jest wykorzystywany do celów innych niż utrzymanie lub poprawa bezpieczeństwa. Korzyści są dwojakie. Często personel jest najbliższym zagrożeniom bezpieczeństwa, więc dobrowolny system zgłaszania pozwala im aktywnie identyfikować te zagrożenia i sugerować możliwe do zastosowania rozwiązania. Jednocześnie władza lotnicza lub kierownictwo są w stanie zebrać ważne informacje bezpieczeństwa i budować zaufanie wśród organizacji lub personelu operacyjnego, który zgłasza informacje. Więcej informacji na temat ochrony danych bezpieczeństwa i informacji bezpieczeństwa znajduje się w Rozdziale 7.

3.2.5.2 Skłonność do zgłaszania swoich doświadczeń i błędów przez organizacje lub osoby w dużej mierze zależy od postrzeganych korzyści i wad związanych ze zgłaszaniem. Systemy zgłaszania zdarzeń związanych z bezpieczeństwem mogą być anonimowe lub poufne. Ogólnie rzecz biorąc, w systemie anonimowym osoba zgłaszająca nie podaje swojej tożsamości. W takim przypadku nie ma możliwości dalszego wyjaśnienia treści zgłoszenia ani możliwości przekazania informacji zwrotnej. W systemie poufnym, wszelkie informacje identyfikujące osobę zgłaszającą są znane tylko wyznaczonemu urzędnikowi. Jeżeli organizacje i osoby, które zgłaszają problemy związane z bezpieczeństwem, są chronione i traktowane w sprawiedliwy i konsekwentny sposób, istnieje większe prawdopodobieństwo, że ujawnią takie informacje i będą współpracować z władzą lotniczą lub kierownictwem w celu skutecznego zarządzania ryzykiem bezpieczeństwa.

3.2.5.3 Od Państw oczekuje się przyjęcia przepisów, które będą zgodne z przepisami zawartymi w Załączniku 19, dotyczącymi ochrony danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł. W przypadku dobrowolnego systemu zgłaszania należy zapewnić poufność oraz działanie systemu zgodnie z przepisami dotyczącymi ochrony bezpieczeństwa. Ponadto organizacje muszą posiadać odpowiednią politykę dyscyplinarną, dostępną dla wszystkich i rozumianą w całej organizacji. Polityka dyscyplinarna powinna jasno wskazywać zachowania uznawane za nieakceptowalne oraz sposób reagowania przez organizację w takich przypadkach. Polityka dyscyplinarna musi być stosowana sprawiedliwie, rozsądnie i konsekwentnie. Wreszcie organizacje i osoby częściej zgłaszają swoje doświadczenia i błędy w środowisku, w którym nie będą oceniane lub traktowane niesprawiedliwie przez swoich współpracowników lub swojego pracodawcę.

3.2.5.4 Ogólnie rzecz biorąc, organizacje i osoby muszą wierzyć, że będą wspierane podczas zgłaszania w interesie bezpieczeństwa. Dotyczy to błędów organizacyjnych i osobistych. Zwiększenie liczby poufnych zgłoszeń i zmniejszenie liczby anonimowych zgłoszeń wskazuje zazwyczaj na postęp organizacji w kierunku pozytywnej kultury bezpieczeństwa.

3.2.6 Kultura bezpieczeństwa i różnorodność kulturowa

3.2.6.1 Kultura narodowa różnicuje cechy poszczególnych narodów, w tym rolę jednostki w społeczeństwie, sposób podziału władzy oraz priorytety krajowe w odniesieniu do zasobów, odpowiedzialności, moralności, celów i systemów prawnych.

3.2.6.2 Z punktu widzenia zarządzania bezpieczeństwem, kultura narodowa wpływa na kulturę organizacyjną i odgrywa dużą rolę w określaniu charakteru i zakresu polityki egzekwowania przepisów, w tym relacji pomiędzy personelem reprezentującym prawo a personelem reprezentującym branżę, oraz zakresu, w jakim informacje bezpieczeństwa są chronione. To z kolei wpływa na chęć ludzi do zgłaszania problemów związanych z bezpieczeństwem.

3.2.6.3 Większość organizacji zatrudnia dziś ludzi z różnych środowisk kulturowych, które mogą być określone przez ich narodowość, pochodzenie etniczne, religię i/lub płeć. Operacje i bezpieczeństwo lotnicze opierają się na skutecznej interakcji między różnymi grupami zawodowymi, z których każda ma własną kulturę zawodową. W związku z tym, znaczący wpływ na kulturę bezpieczeństwa organizacji może również mieć różnorodność środowisk kulturowych jej pracowników.

3.2.6.4 Zarządzanie bezpieczeństwem w systemie lotniczym wymaga zatem interakcji i zarządzania zróżnicowanym kulturowo personelem. Jednak wdrażając zarządzanie bezpieczeństwem, menedżerowie powinni być w stanie formować swoją zróżnicowaną kulturowo siłę roboczą w efektywnie pracujące zespoły. Wyeliminowanie różnic w postrzeganiu ryzyka bezpieczeństwa, które mogą wywodzić się z różnych interpretacji kulturowych, oraz wzmocnienie innych aspektów związanych z bezpieczeństwem, takich jak komunikacja, style przywództwa i interakcja między przełożonymi i podwładnymi mają kluczowe znaczenie. Powodzenie uzależnione jest od zdolności kierownictwa do promowania wspólnego rozumienia bezpieczeństwa i roli odgrywanej przez jednostkę. Niezależnie od pochodzenia kulturowego danej osoby, skuteczne zarządzanie bezpieczeństwem opiera się na wspólnej kulturze bezpieczeństwa, w której wszyscy w organizacji rozumieją, w jaki sposób powinni się zachowywać w odniesieniu do bezpieczeństwa i ryzyka „nawet wtedy, gdy nikt nie patrzy”.

3.2.7 Kultura bezpieczeństwa i zmiana organizacyjna

Zarządzanie bezpieczeństwem wymaga od organizacji zarządzania ryzykami bezpieczeństwa związanymi ze zmianami organizacyjnymi i operacyjnymi. Obawy pracowników dotyczące obciążenia pracą, bezpieczeństwa pracy i dostępu do szkoleń wiążą się ze znaczącą zmianą w organizacji i mogą mieć negatywny wpływ na kulturę bezpieczeństwa. Stopień, w jakim personel czuje się zaangażowany w opracowanie zmiany oraz rozumie swoją rolę w tym procesie, również wpływa na kulturę bezpieczeństwa.

3.3. TWORZENIE POZYTYWNEJ KULTURY BEZPIECZEŃSTWA

3.3.1 Pozytywna kultura bezpieczeństwa ma następujące cechy:

- a) menedżerowie i pracownicy, indywidualnie i zbiorowo, chcą podejmować decyzje i działania promujące bezpieczeństwo;
- b) osoby i grupy nieustannie wyrażają krytykę swoich zachowań i procesów oraz chętnie przyjmują krytykę innych osób pragnących zmiany i poprawy wraz ze zmianami środowiska;

- c) kierownictwo i pracownicy mają wspólną świadomość zagrożeń i ryzyk, przed jakimi stoi organizacja i prowadzona przez nią działalność, oraz świadomość potrzeby zarządzania ryzykami;
- d) poszczególne osoby działają i podejmują decyzje zgodnie ze wspólnym przekonaniem, że bezpieczeństwo stanowi element ich działalności;
- e) poszczególne osoby cenią sobie bycie poinformowanym oraz informowanie innych o bezpieczeństwie;
- f) poszczególne osoby ufają swoim współpracownikom i menedżerom przekazując informacje o swoich doświadczeniach oraz zachęca się do zgłaszania błędów w celu poprawy sposobu postępowania w przyszłości.

3.3.2 Działania kierownictwa i pracowników mogą przyczynić się do zwiększenia pozytywnej kultury bezpieczeństwa. Tabela 5 zawiera przykłady działań ze strony kierownictwa i pracowników, które mogą wspomagać bądź hamować tworzenie pozytywnej kultury bezpieczeństwa w organizacji. Organizacje powinny skupić się na zapewnieniu czynników wspomagających i eliminacji wszelkich czynników hamujących w celu promowania i osiągnięcia pozytywnej kultury bezpieczeństwa.

Tabela 5. Przykłady działań, które wspomagają lub hamują tworzenie pozytywnej kultury bezpieczeństwa

<i>Element</i>	<i>Opis ogólny</i>	<i>Czynniki wspomagające</i>	<i>Czynniki hamujące</i>
Zaangażowanie w bezpieczeństwo			
Zaangażowanie w bezpieczeństwo odzwierciedla zakres, w jakim kierownictwo wyższego szczebla w organizacji ma pozytywne nastawienie do bezpieczeństwa i uznaje jego znaczenie. Kierownictwo wyższego szczebla powinno być szczerze zaangażowane w osiąganie i utrzymywanie wysokiego poziomu bezpieczeństwa oraz motywowanie pracowników i zapewnianie im środków dla tego celu.	<ul style="list-style-type: none"> • Kierownictwo angażuje się w tworzenie kultury bezpieczeństwa i motywuje pracowników do dbania o bezpieczeństwo, nie tylko poprzez mówienie, ale również działanie jako wzór do naśladowania. • Kierownictwo zapewnia zasoby dla szeregu zadań związanych z bezpieczeństwem (np. szkolenia). • Ustanowiono stały nadzór i kierowanie w odniesieniu do zarządzania bezpieczeństwem. 	<ul style="list-style-type: none"> • Kierownictwo demonstruje, że zysk, ograniczanie kosztów oraz wydajność są najważniejsze. • Inwestycje mające na celu poprawę bezpieczeństwa są często podejmowane kiedy wymagają tego przepisy lub po wystąpieniu wypadku. • Nie ustanowiono nadzoru ani kierowania w odniesieniu do zarządzania bezpieczeństwem. 	
Zdolność adaptacji			
Zdolność adaptacji odzwierciedla zakres, w jakim pracownicy i kierownictwo są gotowi wyciągnąć wnioski z doświadczeń z przeszłości oraz zakres, w jakim są w stanie podjąć niezbędne działania w celu podniesienia poziomu bezpieczeństwa w organizacji.	<ul style="list-style-type: none"> • Pracownicy są zachęceni do aktywnego udziału w rozwiązywaniu problemów związanych z bezpieczeństwem. • Wszystkie incydenty oraz ustalenia z audytów są badane i na ich podstawie podejmowane są działania. 	<ul style="list-style-type: none"> • Wkład pracowników w problemy związane z bezpieczeństwem nie jest poszukiwany na wszystkich poziomach pracowników. • Działania są często podejmowane 	

	<ul style="list-style-type: none"> • Procesy i procedury organizacyjne są sprawdzane pod względem ich wpływu na bezpieczeństwo (wysoki stopień samokrytycyzmu). • Proaktywne podejście do bezpieczeństwa jest demonstrowane i realizowane. 	<p>jedynie po wystąpieniu wypadków lub gdy wymagają tego przepisy.</p> <ul style="list-style-type: none"> • Procesy i procedury organizacyjne uznaje się za odpowiednie, dopóki nie nastąpi wypadek (samozadowolenie lub brak samokrytycyzmu) • Nawet gdy zdarzy się wypadek, organizacja jest niechętna do sprawdzania samej siebie. • Reaktywne podejście do bezpieczeństwa jest demonstrowane i realizowane.
Świadomość		
<p>Świadomość odzwierciedla zakres, w jakim pracownicy i kierownictwo są świadomi ryzyk lotniczych, z jakimi boryka się organizacja oraz prowadzona przez nią działalność.</p> <p>Z perspektywy Państwa pracownicy są świadomi zarówno ryzyka bezpieczeństwa wynikającego z ich własnej działalności, jak i organizacji, które nadzorują. Pracownicy i kierownictwo powinni stale utrzymywać wysoki stopień czujności w odniesieniu do problemów związanych z bezpieczeństwem.</p>	<ul style="list-style-type: none"> • Ustanowiono skuteczny sposób identyfikacji zagrożeń. • Dochodzenia mają na celu ustalenie zasadniczej przyczyny zdarzenia. • Organizacja pozostaje na bieżąco z istotnymi usprawnieniami w zakresie bezpieczeństwa, i w razie konieczności wprowadza odpowiednie modyfikacje. • Organizacja systematycznie ocenia, czy usprawnienia w zakresie bezpieczeństwa są wdrażane i czy działają zgodnie z założeniami. • W stosownych przypadkach członkowie organizacji są świadomi ryzyk bezpieczeństwa wynikających z ich indywidualnych działań i operacji/działalności firmy. 	<ul style="list-style-type: none"> • Nie podejmuje się żadnych wysiłków na rzecz identyfikacji zagrożeń. • Dochodzenia są realizowane do momentu wykrycia pierwszej możliwej przyczyny, a nie skupiają się na szukaniu zasadniczej przyczyny. • Organizacja nie jest na bieżąco z istotnymi usprawnieniami w zakresie bezpieczeństwa. • Organizacja nie ocenia, czy usprawnienia w zakresie bezpieczeństwa są wdrażane we właściwy sposób. • W stosownych przypadkach członkowie organizacji nie są świadomi ryzyk bezpieczeństwa wynikających z ich indywidualnych

		<p>działań i operacji firmy.</p> <ul style="list-style-type: none"> Dane bezpieczeństwa są gromadzone, ale nie są analizowane, i na ich podstawie nie są podejmowane żadne działania.
Zachowanie w odniesieniu do bezpieczeństwa		
<p>Zachowanie w odniesieniu do bezpieczeństwa odzwierciedla zakres, w jakim każdy poziom organizacji zachowuje się w taki sposób, aby utrzymać i poprawić poziom bezpieczeństwa. Znaczenie bezpieczeństwa powinno być uznane oraz procesy i procedury konieczne do jego utrzymania powinny być wdrożone.</p>	<ul style="list-style-type: none"> Pracownicy motywują się wzajemnie do bezpiecznego działania oraz poprzez działają jako wzór do naśladowania. Prowadzone jest ciągle monitorowanie bezpiecznego zachowania. Celowe niebezpieczne zachowanie nie jest tolerowane przez kierownictwo i współpracowników. Warunki pracy nieprzerwanie wspierają bezpieczeństwo lotnicze. 	<ul style="list-style-type: none"> Pracownicy nie są karani za umyślne niebezpieczne zachowanie dla własnych korzyści lub innych interesów. Warunki pracy prowokują zachowanie i działania, które są szkodliwe dla bezpieczeństwa lotniczego. Nie jest praktykowane monitorowanie bezpieczeństwa lotniczego w ramach produktów lub usług organizacji. Konstruktywna krytyka na rzecz bezpieczeństwa lotniczego nie jest mile widziana.
Informacja		
<p>Informacje odzwierciedlają zakres, w jakim informacje są przekazywane wszystkim niezbędnym osobom w organizacji. Pracownicy powinni być włączeni i zachęceni do zgłaszania obaw związanych z bezpieczeństwem lotniczym oraz otrzymywać informacje zwrotne na temat swoich zgłoszeń. Informacje o pracy związane z bezpieczeństwem lotniczym muszą być przekazywane z rozważą do właściwych osób, aby uniknąć nieporozumień, które mogłyby prowadzić do niebezpiecznych sytuacji i konsekwencji w systemie lotniczym.</p> <p>Państwo jest otwarte na udostępnianie informacji dotyczących bezpieczeństwa lotniczego wszystkim podmiotom prowadzącym działalność w lotnictwie cywilnym.</p>	<ul style="list-style-type: none"> Istnieje otwarte i sprawiedliwe środowisko zgłaszania zdarzeń związanych z bezpieczeństwem. Pracownicy otrzymują informacje bezpieczeństwa w odpowiednim czasie, aby umożliwić prowadzenie bezpiecznych operacji lub podjęcie odpowiednich decyzji. Kierownictwo i przełożeni regularnie sprawdzają, czy informacje bezpieczeństwa są zrozumiałe i czy na ich podstawie podejmowane są działania. Aktywnie praktykowany jest transfer wiedzy i szkoleń w zakresie 	<ul style="list-style-type: none"> Oczywiste jest środowisko zgłaszania zdarzeń związanych z bezpieczeństwem, w którym przypisywana jest wina. Informacje bezpieczeństwa są wstrzymywane. Komunikacja w zakresie bezpieczeństwa nie jest monitorowana pod kątem jej skuteczności. Nie zapewnia się transferu wiedzy ani szkoleń.

	bezpieczeństwa lotniczego (np. wymiana zdobytych doświadczeń).	
Zaufanie		
<p>Wkład pracowników w bezpieczeństwo rozwija środowisko zgłaszania zdarzeń związanych z bezpieczeństwem, które sprzyja zaufaniu - zaufaniu, że ich działania lub zaniechania, współmierne do ich szkolenia i doświadczenia, nie będą karane. Praktycznym podejściem jest zastosowanie testu racjonalności - tzn. czy uzasadnione jest, aby osoba o tym samym poziomie doświadczenia i szkolenia mogła zrobić to samo. Takie środowisko ma fundamentalne znaczenie dla skutecznego i wydajnego zgłaszania zdarzeń związanych z bezpieczeństwem.</p> <p>Skuteczne systemy zgłaszania zdarzeń związanych z bezpieczeństwem pomagają zapewnić, że ludzie są gotowi do zgłaszania swoich błędów i doświadczeń, tak aby Państwa i podmioty prowadzące działalność w lotnictwie cywilnym miały dostęp do odpowiednich danych i informacji, które są niezbędne do rozwiązania istniejących i potencjalnych niedoskonałości oraz zagrożeń w zakresie bezpieczeństwa. Systemy te tworzą środowisko, w którym ludzie mogą być pewni, że dane oraz informacje bezpieczeństwa będą wykorzystywane wyłącznie w celu poprawy bezpieczeństwa.</p>	<ul style="list-style-type: none"> Istnieje rozróżnienie pomiędzy zachowaniem akceptowalnym a nieakceptowalnym, które jest znane wszystkim pracownikom. Badania zdarzeń (w tym wypadków i incydentów) uwzględniają czynniki indywidualne i organizacyjne. Dobry poziom bezpieczeństwa lotniczego jest rozpoznawany i regularnie nagradzany. Istnieje chęć wśród pracowników i personelu operacyjnego do zgłaszania zdarzeń, w które byli oni zaangażowani. 	<ul style="list-style-type: none"> Nie ma wyraźnego rozróżnienia pomiędzy zachowaniem akceptowalnym i nieakceptowalnym. Pracownicy są systematycznie i rygorystycznie karani za błędy ludzkie. Badania wypadków i zdarzeń koncentrują się tylko na indywidualnych czynnikach. Dobry poziom bezpieczeństwa i bezpieczne zachowanie są traktowane jak coś oczywistego.

3.3.3 Monitorowanie kultury bezpieczeństwa

3.3.3.1 Kultura bezpieczeństwa podlega wielu wpływom i organizacje mogą zdecydować się na ocenę swojej kultury bezpieczeństwa w celu:

- zrozumienia sposobu, w jaki ludzie postrzegają organizację i znaczenie bezpieczeństwa;
- zidentyfikowania mocnych i słabych stron;
- zidentyfikowania różnic pomiędzy różnymi grupami (subkulturami) w obrębie organizacji; oraz
- zbadania zmian mających miejsce wraz z upływem czasu (np. w odpowiedzi na znaczące zmiany organizacyjne, np. w następstwie wypadku, zmiany w kierownictwie wyższego szczebla lub zmiany układu stosunków przemysłowych).

3.3.3.2 Istnieje szereg narzędzi służących do oceny dojrzałości kultury bezpieczeństwa, zazwyczaj w połączeniu:

- kwestionariusze;
- wywiady i grupy fokusowe;
- obserwacje; oraz

d) przeglądy dokumentów.

3.3.3.3 Ocena dojrzałości kultury bezpieczeństwa może dostarczyć cennych spostrzeżeń, przyczyniając się do działań ze strony kierownictwa, które zachęcą do pożądaných zachowań bezpieczeństwa. Należy zauważyć, że takie oceny mają pewien stopień subiektywności i mogą odzwierciedlać poglądy oraz postrzeganie sytuacji przez osoby zaangażowane w dane działania tylko w określonym momencie. Również ocena dojrzałości kultury bezpieczeństwa może mieć niezamierzone konsekwencje w postaci nieumyślnego zachęcania organizacji do osiągnięcia „właściwego” wyniku, zamiast współpracy w celu zrozumienia i poprawy kultury bezpieczeństwa.

ROZDZIAŁ 4

ZARZĄDZANIE POZIOMEM BEZPIECZEŃSTWA

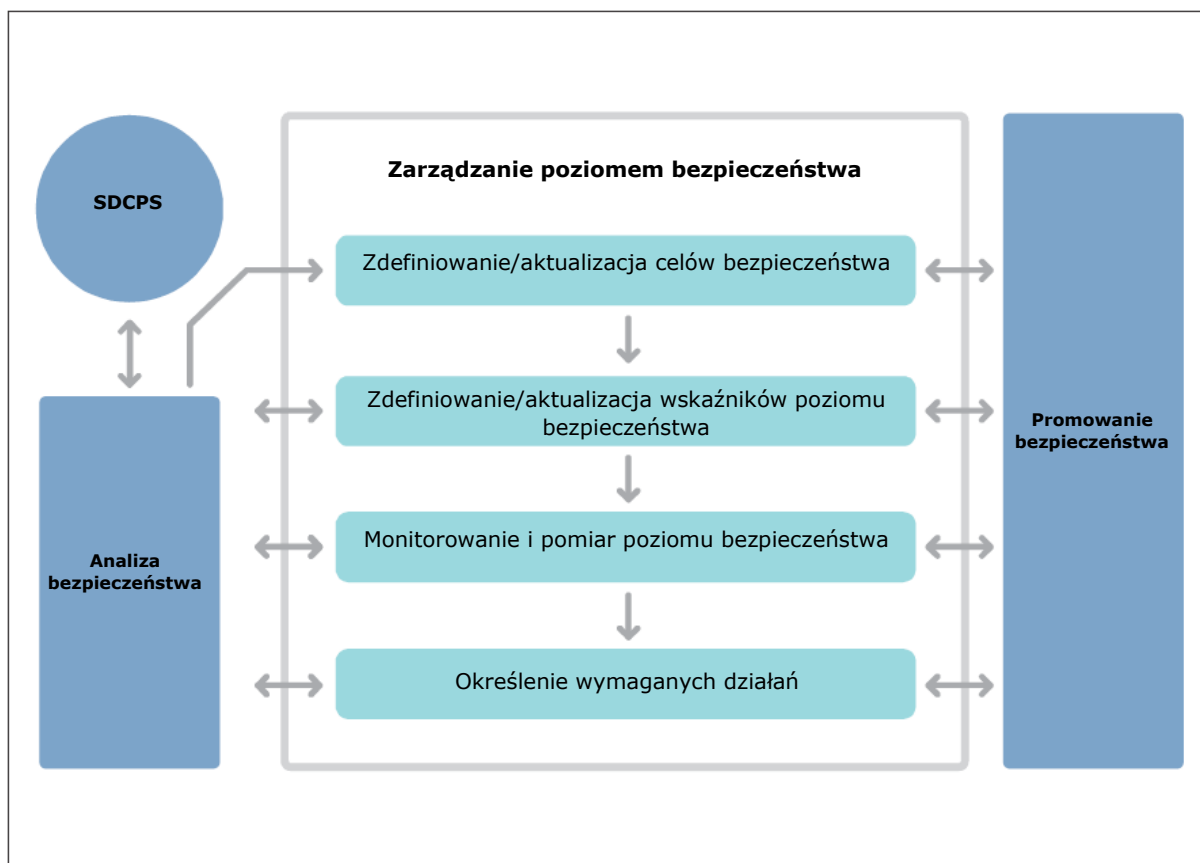
4.1. WSTĘP

4.1.1 Zarządzanie poziomem bezpieczeństwa ma kluczowe znaczenie dla funkcjonowania krajowych programów bezpieczeństwa (SSP) i systemów zarządzania bezpieczeństwem (SMS). Odpowiednio wdrożone zapewni organizacji środki pozwalające określić, czy jej działania i procesy są skutecznie, aby osiągnąć cele bezpieczeństwa. Jest to osiągnięte poprzez identyfikację wskaźników poziomu bezpieczeństwa (SPI), które są używane do monitorowania i pomiaru bezpieczeństwa. Dzięki identyfikacji wskaźników SPI, uzyskane informacje pozwolą kierownictwu wyższego szczebla na zapoznanie się z bieżącą sytuacją i wsparcie procesu decyzyjnego, w tym określenie, czy konieczne są działania w celu dalszego ograniczenia ryzyk bezpieczeństwa, aby zapewnić osiągnięcie celów bezpieczeństwa przez organizację.

4.1.2 Ogólny proces zarządzania poziomem bezpieczeństwa oraz sposób, w jaki jest on powiązany z systemami zbierania i przetwarzania danych bezpieczeństwa (SDCPS) oraz analizą bezpieczeństwa, omówiony w Rozdziale 5 i 6, odpowiednio, przedstawiony został na Rysunku 4-1 poniżej. Powiązanie z promocją bezpieczeństwa podkreśla znaczenie przekazywania tych informacji w obrębie całej organizacji. Więcej informacji na temat promocji bezpieczeństwa, będącej ważnym elementem SSP i SMS, często niedocenianym, znajduje się w Rozdziale 8 i 9, odpowiednio.

4.1.3 Zarządzanie poziomem bezpieczeństwa pomaga organizacji sformułować pytania i odpowiedzi dotyczące czterech najważniejszych zagadnień dotyczących zarządzania bezpieczeństwem:

- a) Jakie są główne ryzyka bezpieczeństwa organizacji? *Ryzyka opracowane na podstawie przeglądu danych o wypadkach i incydentach lotniczych oraz analizy prognostycznej prowadzonej w celu zidentyfikowania i zdefiniowania pojawiających się ryzyk.*
- b) Co organizacja chce osiągnąć pod względem bezpieczeństwa i jakie są najważniejsze ryzyka bezpieczeństwa, które należy uwzględnić? *Cele bezpieczeństwa organizacji.*
- c) W jaki sposób organizacja będzie wiedzieć, czy robi postępy w kierunku realizacji celów bezpieczeństwa? *Poprzez SPI, SPT i, jeżeli to możliwe, czynniki uruchamiające bezpieczeństwo.*
- d) Jakie dane bezpieczeństwa i informacje bezpieczeństwa są potrzebne do podejmowania świadomych decyzji w zakresie bezpieczeństwa, w tym dotyczących alokacji zasobów organizacji? *Dane/informacje uzyskane dzięki systemowi zbierania i przetwarzania danych dotyczących bezpieczeństwa (SDCPS) i analizie danych dotyczących bezpieczeństwa.*



Rysunek 4-1. Proces zarządzania poziomem bezpieczeństwa

4.1.4 Proces zarządzania poziomem bezpieczeństwa może być również wykorzystany do ustanowienia akceptowalnego poziomu bezpieczeństwa (ALoSP). Więcej szczegółowych informacji na temat ustanowienia ALoSP znajduje się w Rozdziale 8.

4.1.5 Relacje pomiędzy Państwami a podmiotami lotniczymi

4.1.5.1 Istnieją podobieństwa pomiędzy Państwem a podmiotami lotniczymi w zakresie wykorzystania i stosowania technik bezpieczeństwa. Podczas gdy wytyczne zawarte w niniejszym rozdziale zostały opracowane zarówno dla Państw, jak i dla podmiotów, w niniejszej części zidentyfikowano pewne różnice.

4.1.5.2 Opracowanie poziomu bezpieczeństwa Państwa powinno koncentrować się na tym, co Państwo uważa za najważniejszy aspekt zarządzania bezpieczeństwem. Dla Państwa, efektywnie wdrożony krajowy program bezpieczeństwa jest wykorzystywany jako narzędzie do podejmowania decyzji w zakresie zarządzania poziomem bezpieczeństwa, który powinien obejmować: poziom bezpieczeństwa podmiotów lotniczych, zdolność Państwa do sprawowania nadzoru, oraz wsparcie dla podmiotów poprzez ustanowienie wytycznych. Państwa powinny rozważyć określenie swoich zdolności do:

- a) utrzymania systemu nadzoru nad bezpieczeństwem;
- b) stosowania określonych działań w zakresie bezpieczeństwa i wprowadzania inicjatyw w zakresie bezpieczeństwa; oraz
- c) dostosowania istniejących środków kontroli ryzyka bezpieczeństwa w celu zapewnienia ich skuteczności.

4.1.5.3 W przypadku podmiotu lotniczego, podstawową funkcją zarządzania poziomem bezpieczeństwem jest monitorowanie i mierzenie, w jakim stopniu zarządza on ryzykiem bezpieczeństwa. Jest to osiągane dzięki skutecznemu wdrożeniu systemu SMS, który generuje informacje, które będą wykorzystywane do podejmowania decyzji dotyczących zarządzania bezpieczeństwem, w tym wdrożenia środków kontroli ryzyka bezpieczeństwa i alokacji zasobów.

4.1.5.4 Sukces zarządzania bezpieczeństwem zależy od zaangażowania Państwa i jego podmiotów lotniczych. Identyfikowanie przez Państwo wskaźników SPI może być korzystne, ponieważ mogą one być monitorowane przez podmioty, a następnie udostępniane Państwu, w szczególności w celu ustanowienia akceptowalnego poziomu bezpieczeństwa (ALoSP) (patrz Rozdział 8, aby uzyskać więcej informacji). Informacje otrzymane od podmiotów lotniczych pomogą Państwu w ocenie poziomu bezpieczeństwa branży lotniczej oraz jego własnej zdolności do zapewnienia skutecznego nadzoru i wsparcia podmiotów. Jednak podmioty lotnicze powinny zapewnić, że ich wskaźniki poziomu bezpieczeństwa są odpowiednie do ich kontekstu operacyjnego, historii i oczekiwania.

4.1.6 Zarządzanie poziomem bezpieczeństwa i interfejsy

4.1.6.1 Kiedy Państwa i podmioty lotnicze rozważają wdrożenie zarządzania bezpieczeństwem, ważne jest, aby wziąć pod uwagę ryzyka bezpieczeństwa powodowane przez podmioty powiązane. Interfejsy mogą mieć charakter wewnętrzny (np. pomiędzy operacjami i obsługą techniczną lub działami finansowymi, zasobami ludzkimi lub działami prawnymi) lub zewnętrzny (np. inne Państwo, podmioty prowadzące działalność w lotnictwie cywilnym i podwykonawcy). Zagrożenia i związane z nimi ryzyka w punktach interfejsu należą do najczęstszych czynników sprawczych zdarzeń związanych z bezpieczeństwem. Państwa i podmioty mają większą kontrolę nad ryzykami związanymi z interfejsami, kiedy ich interfejsy są identyfikowane i zarządzane. Interfejsy należy zdefiniować w opisie systemu organizacji.

4.1.6.2 Państwa i podmioty lotnicze są odpowiedzialne za bieżące monitorowanie i zarządzanie swoimi interfejsami w celu zapewnienia bezpiecznej działalności. Ryzyko bezpieczeństwa, jakie stwarza każdy interfejs, powinno być wspólnie oceniane przez podmioty powiązane. Współpraca jest wysoce pożądana, ponieważ postrzeganie ryzyk bezpieczeństwa i ich tolerowanie mogą się różnić w zależności od organizacji powiązanych. Dzielenie się zarządzaniem ryzykiem związanym z interfejsami, poprzez ustanowienie i monitorowanie wskaźników SPI, sprzyja wzajemnej świadomości ryzyk bezpieczeństwa, a nie ignorancji lub potencjalnie jednostronnemu zarządzaniu ryzykiem. Stwarza także możliwość transferu wiedzy i praktyk roboczych, które mogłyby poprawić skuteczność bezpieczeństwa obydwu organizacji.

4.1.6.3 Z tego powodu, należy uzgodnić i ustanowić wskaźniki SPI w celu monitorowania i pomiaru ryzyka oraz skuteczności działań łagodzących. Oficjalna umowa dotycząca zarządzania interfejsami zawarta pomiędzy organizacjami powiązanimi, z jasno określonymi obowiązkami w zakresie monitorowania i zarządzania, stanowi przykład skutecznego podejścia.

4.2. CELE BEZPIECZEŃSTWA

4.2.1 Cele bezpieczeństwa to krótkie oświadczenia o charakterze ogólnym dotyczące osiągnięć w zakresie bezpieczeństwa lub pożądanego wyników, które należy uzyskać. Cele bezpieczeństwa wyznaczają kierunek działań organizacji i dlatego powinny być spójne z polityką bezpieczeństwa, która określa wysoki poziom zaangażowania organizacji w bezpieczeństwo. Cele są również przydatne do przekazywania priorytetów bezpieczeństwa personelowi i społeczności lotniczej jako całości. Ustanowienie celów bezpieczeństwa zapewnia strategiczny kierunek procesu zarządzania poziomem bezpieczeństwa i zapewnia solidną podstawę do podejmowania decyzji związanych z bezpieczeństwem. Zarządzanie poziomem bezpieczeństwa powinno stanowić podstawowy czynnik do uwzględnienia podczas zmiany zasad lub procesów lub podczas przydzielania zasobów organizacji w celu poprawy poziomu bezpieczeństwa.

4.2.2 Cele bezpieczeństwa mogą być:

- a) *ukierunkowane na proces*: określone w kategoriach bezpiecznych zachowań, jakich oczekuje się od personelu operacyjnego lub wykonania działań wdrożonych przez organizację w celu zarządzania ryzykiem bezpieczeństwa; lub
- b) *ukierunkowane na wynik*: obejmuje działania i trendy dotyczące ograniczania wypadków lub strat operacyjnych.

4.2.3 Pakiet celów bezpieczeństwa powinien obejmować połączenie zarówno celów ukierunkowanych na proces, jak i celów ukierunkowanych na wynik w celu zapewnienia dostatecznego zasięgu i kierunku dla SPI i SPT. Cele bezpieczeństwa same w sobie nie muszą być konkretne, wymierne, osiągalne, istotne i aktualne (SMART) (George T. Doran, 1981), pod warunkiem, że cele w zakresie bezpieczeństwa i towarzyszące im SPI i SPT tworzą pakiet, który pozwala organizacji wykazać, czy utrzymuje lub poprawia swój poziom bezpieczeństwa.

Tabela 6. Przykłady celów bezpieczeństwa

<i>Przykłady celów bezpieczeństwa</i>		
ukierunkowane na proces	Państwo lub podmiot lotniczy	Zwiększyć poziom zgłaszania zdarzeń związanych z bezpieczeństwem.
ukierunkowane na wynik	podmiot lotniczy	Zmniejszyć wskaźnik niepożądanych zdarzeń związanych z bezpieczeństwem na płycie. lub Zmniejszyć roczną liczbę niepożądanych zdarzeń związanych z bezpieczeństwem na płycie w stosunku do poprzedniego roku.
ukierunkowane na wynik	Państwo	Zmniejszyć roczną liczbę zdarzeń związanych z bezpieczeństwem w sektorze X

4.2.4 Organizacja może również zdecydować się na określenie celów bezpieczeństwa na poziomie taktycznym lub operacyjnym lub zastosować je do konkretnych projektów, produktów i procesów. Cel bezpieczeństwa może być również wyrażony poprzez użycie innych terminów o podobnym znaczeniu.

4.3. WSKAŹNIKI POZIOMU BEZPIECZEŃSTWA (SPI) I CELE POZIOMÓW BEZPIECZEŃSTWA (SPT)

4.3.1 Rodzaje wskaźników poziomu bezpieczeństwa

Wskaźniki jakościowe i ilościowe

4.3.1.1 Wskaźniki SPI są używane, aby zapewnić kierownictwu wyższego szczebla wiedzę, czy organizacja może osiągnąć swój cel bezpieczeństwa. Wskaźniki mogą być jakościowe lub ilościowe. Wskaźniki ilościowe odnoszą się do pomiaru poprzez ilość, nie jakość, podczas gdy wskaźniki jakościowe mają charakter opisowy i dokonują pomiaru poprzez jakość. Wskaźniki ilościowe są preferowane bardziej aniżeli wskaźniki jakościowe, ponieważ łatwiej je policzyć i porównać. Wybór wskaźnika zależy od dostępności wiarygodnych danych, które można zmierzyć ilościowo. Czy konieczne dowody muszą mieć formę porównywalnych, uogólnionych danych (ilościowych) lub opisowego obrazu sytuacji w zakresie bezpieczeństwa (jakościowego)? Każda opcja, jakościowa lub ilościowa, obejmuje różne rodzaje wskaźników SPI i wymaga przemyślanego procesu wyboru SPI. Połączenie podejść jest przydatne w wielu sytuacjach i może rozwiązać wiele problemów, które mogą pojawić się w przypadku przyjęcia

jednego podejścia. Przykładem jakościowego wskaźnika dla Państwa może być dojrzałość systemu SMS podmiotów lotniczych w danym sektorze, lub dla podmiotu, ocena kultury bezpieczeństwa.

4.3.1.2 Wskaźniki ilościowe można wyrazić w postaci liczby (x wtargnięć) lub jako współczynnik (x wtargnięć na n operacji). W niektórych przypadkach wystarczające będzie wyrażenie liczbowe. Jednak samo użycie liczb może stworzyć zniekształcony obraz rzeczywistej sytuacji w zakresie bezpieczeństwa, jeżeli poziom działań ulega zmianie. Na przykład, jeżeli kontrola ruchu lotniczego odnotuje trzy przypadki naruszeń nakazanego poziomu lotu w lipcu i sześć przypadków w sierpniu, może istnieć duża obawa o znaczne pogorszenie poziomu bezpieczeństwa. Ale w sierpniu odnotowano podwojenie liczby operacji w porównaniu do lipca, co oznacza, że liczba naruszeń poziomu lotu spadła, a nie wzrosła. Może to wpłynąć na zmianę poziomu kontroli, chociaż nie musi, ale stanowi kolejną cenną informację, która może być istotna dla podejmowania decyzji dotyczących bezpieczeństwa w oparciu o dane.

4.3.1.3 Z tego powodu, w stosownych przypadkach, wskaźniki SPI powinny być odzwierciedlone w kategoriach względnego współczynnika w celu pomiaru poziomu wydajności bez względu na poziom działań. Zapewnia to znormalizowany pomiar wydajności; niezależnie od tego czy poziom działań wzrasta czy maleje. Kolejny przykład to wskaźnik SPI, który może mierzyć liczbę nieuprawnionych wtargnięć na drogę startową. Ale jeżeli w monitorowanym okresie było mniej odlotów, wynik może być mylący. Bardziej dokładną i cenną miarą działań byłaby liczba nieuprawnionych wtargnięć na drogę startową w stosunku do liczby operacji, np. x wtargnięć na 1 000 operacji.

Wskaźniki reaktywne i wskaźniki wiodące

4.3.1.4 Dwie najbardziej popularne kategorie stosowane przez Państwa i podmioty lotnicze do klasyfikacji SPI to wskaźniki reaktywne i wskaźniki wiodące. Reaktywne wskaźniki SPI mierzą zdarzenia, które już miały miejsce. Określane są również jako „wskaźniki SPI oparte na wynikach” i zazwyczaj (ale nie zawsze) dotyczą negatywnych skutków, których organizacja zamierza uniknąć. Wiodące wskaźniki SPI mierzą procesy i dane wejściowe wdrażane w celu poprawy lub utrzymania bezpieczeństwa. Znane są one również jako „wskaźniki SPI odnoszące się do działania lub procesu”, ponieważ monitorują i mierzą warunki, które mogą prowadzić do specyficznego wyniku.

4.3.1.5 Reaktywne wskaźniki SPI pomagają organizacji zrozumieć, co wydarzyło się w przeszłości i są przydatne w określaniu trendów długoterminowych. Mogą być używane jako wskaźnik ogólny lub jako wskazanie konkretnych rodzajów zdarzeń lub lokalizacji, takich jak „rodzaje wypadków na typ statku powietrznego” lub „konkretne rodzaje incydentów według regionu”. Ponieważ reaktywne wskaźniki SPI mierzą wyniki w zakresie bezpieczeństwa, mogą one mierzyć skuteczność działań łagodzących. Wskaźniki te są skuteczne w potwierdzaniu ogólnej wydajności systemu. Na przykład monitorowanie „liczby kolizji na płycie na liczbę operacji pomiędzy pojazdami po przeprojektowaniu oznakowania poziomego na płycie” stanowi miarę skuteczności nowego oznakowania (zakładając, że nic innego się nie zmieniło). Zmniejszenie kolizji potwierdza poprawę ogólnego poziomu bezpieczeństwa na płycie, którą można przypisać danej zmianie.

4.3.1.6 Trendy w reaktywnych wskaźnikach SPI można analizować w celu określenia warunków istniejących w systemie, które należy rozwiązać. Korzystając z poprzedniego przykładu, rosnący trend w kolizjach na płycie na liczbę operacji mógł doprowadzić do identyfikacji działania łagodzącego w postaci oznakowania poziomego płyty.

4.3.1.7 Reaktywne wskaźniki SPI dzieli się na dwa typy:

- a) *małe prawdopodobieństwo/duża dotkliwość*: wyniki to wypadki lub poważne incydenty. Mała częstotliwość wyników o dużej dotkliwości oznacza, że agregacja danych (na poziomie branży lub regionu) może prowadzić do bardziej znaczących analiz. Przykładem tego typu reaktywnego wskaźnika SPI byłoby „uszkodzenie statku powietrznego i/lub silnika w wyniku zderzenia z ptakami”.

- b) *duże prawdopodobieństwo/miała dotkliwość*: wyniki, które niekoniecznie przejawiają się w poważnym wypadku lub incydencie, są one czasami nazywane wskaźnikami prekursorowymi. Wskaźniki SPI dla wyników o dużym prawdopodobieństwie/malej dotkliwości są przede wszystkim wykorzystywane do monitorowania konkretnych problemów związanych z bezpieczeństwem i pomiaru skuteczności istniejących środków łagodzących ryzyko bezpieczeństwa. Przykładem tego typu prekursorowego wskaźnika SPI będzie „wykrycie ptaków przez radar”, który wskazuje poziom aktywności ptaków, a nie ilość rzeczywistych zderzeń z ptakami.

4.3.1.8 W przeszłości środki bezpieczeństwa lotniczego były tendencyjne w stosunku do wskaźników SPI, które odzwierciedlają wyniki „o małym prawdopodobieństwie/dużej dotkliwości”. Jest to zrozumiałe, ponieważ wypadki i poważne incydenty są wydarzeniami o dużym znaczeniu i są łatwe do policzenia. Z perspektywy zarządzania poziomem bezpieczeństwa istnieją jednak wady polegające na nadmiernym poleganiu na wypadkach i poważnych incydentach jako wiarygodnym wskaźniku poziomu bezpieczeństwa. Na przykład wypadki i poważne incydenty są rzadkie (w ciągu roku może się zdarzyć tylko jeden wypadek lub żaden), co utrudnia przeprowadzenie analizy statystycznej w celu zidentyfikowania trendów. Nie musi to oznaczać, że system jest bezpieczny. Konsekwencją polegania na tego rodzaju danych daje potencjalnie fałszywe poczucie pewności, że poziom bezpieczeństwa organizacji lub systemu jest skuteczny, kiedy w rzeczywistości może być niebezpiecznie blisko wystąpienia wypadku.

4.3.1.9 Wskaźniki wiodące to środki, które koncentrują się na procesach i danych wejściowych, które są wdrażane w celu poprawy lub utrzymania bezpieczeństwa. Znane są one również jako „wskaźniki SPI odnoszące się do działania lub procesu”, ponieważ monitorują i mierzą warunki, które mogą prowadzić do specyficznego wyniku.

4.3.1.10 Przykłady wiodących wskaźników SPI dotyczących rozwoju zdolności organizacji do proaktywnego zarządzania poziomem bezpieczeństwa obejmują takie kwestie, jak „odsetek pracowników, którzy pomyślnie ukończyli szkolenie w zakresie bezpieczeństwa na czas” lub „częstotliwość działań związanych z odstraszeniem ptaków”.

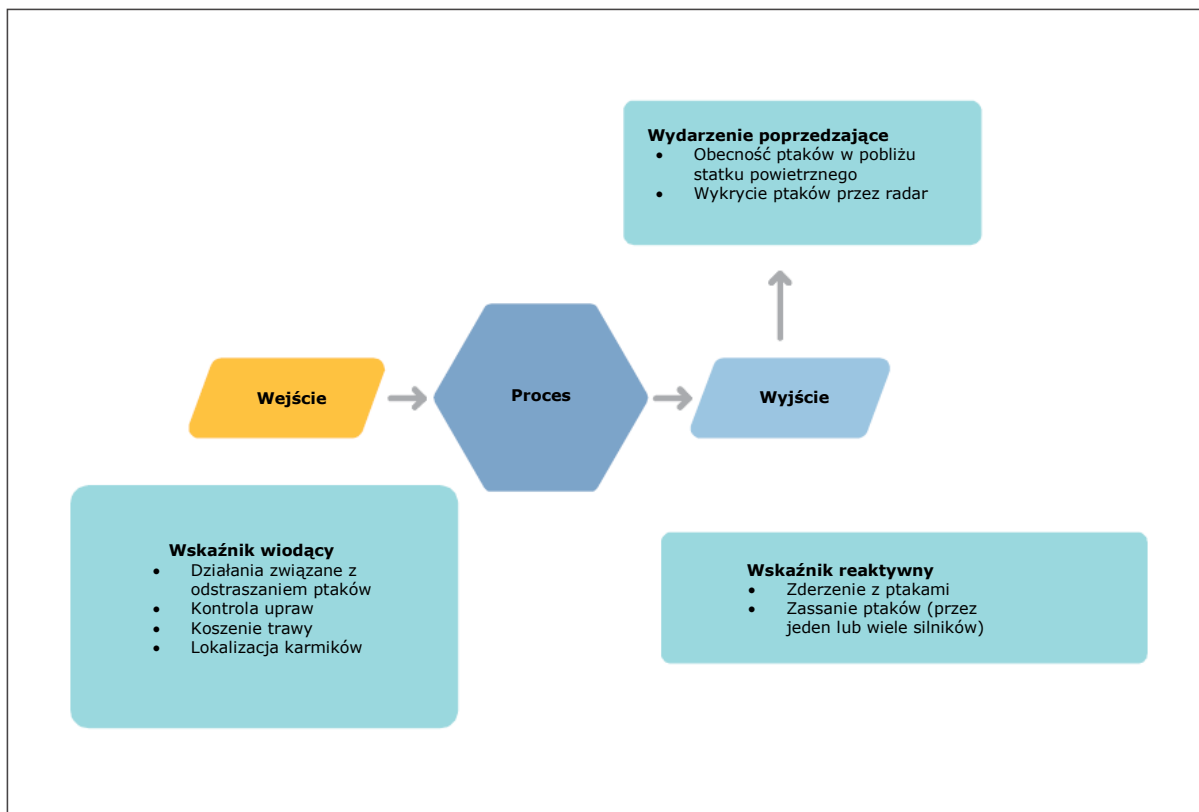
4.3.1.11 Wiodące wskaźniki SPI mogą również być źródłem informacji dla organizacji o tym, jak ich działalność radzi sobie ze zmianami, w tym zmianami w środowisku operacyjnym. Nacisk zostanie położony na przewidywanie słabych punktów w wyniku wprowadzenia zmiany, lub na monitorowanie działania po wprowadzeniu zmiany. Przykładem wskaźnika SPI mającym za zadanie monitorowanie zmiany w operacjach byłby „odsetek miejsc, które wdrożyły procedurę X”.

4.3.1.12 W celu uzyskania bardziej dokładnego i użytecznego wskazania poziomu bezpieczeństwa, reaktywne wskaźniki SPI mierzące zarówno zdarzenia o „małym prawdopodobieństwie/dużej dotkliwości” jak i zdarzenia o „dużym prawdopodobieństwie/malej dotkliwości” powinny być połączone z wiodącymi wskaźnikami SPI. Rysunek 4-2 przedstawia koncepcję wskaźników reaktywnych i wiodących, które zapewniają bardziej kompleksowy i realistyczny obraz poziomu bezpieczeństwa organizacji.

4.3.2 Wybór i definiowanie wskaźników poziomu bezpieczeństwa (SPI)

4.3.2.1 Wskaźniki SPI to parametry, które zapewniają organizacji ogólny obraz jej poziomu bezpieczeństwa w przeszłości, teraźniejszości oraz w odniesieniu do przyszłości. Obraz ten działa jako solidna i dająca się obronić podstawa, na której podejmowane są decyzje w zakresie bezpieczeństwa organizacji w oparciu o dane. Decyzje te z kolei pozytywnie wpływają na poziom bezpieczeństwa organizacji. Identyfikacja wskaźników SPI powinna zatem być realistyczna, odpowiednia i powiązana z celami bezpieczeństwa, niezależnie od ich prostoty lub złożoności.

4.3.2.2 Prawdopodobnie początkowy wybór wskaźników SPI będzie ograniczony do monitorowania i pomiaru parametrów reprezentujących zdarzenia lub procesy, które są łatwe i/lub wygodne do wychwycenia (dane bezpieczeństwa, które mogą być łatwo dostępne). Najlepiej gdyby wskaźniki SPI skupiały się na parametrach, które są ważnymi wskaźnikami poziomu bezpieczeństwa, a nie na tych, które są łatwe do osiągnięcia.

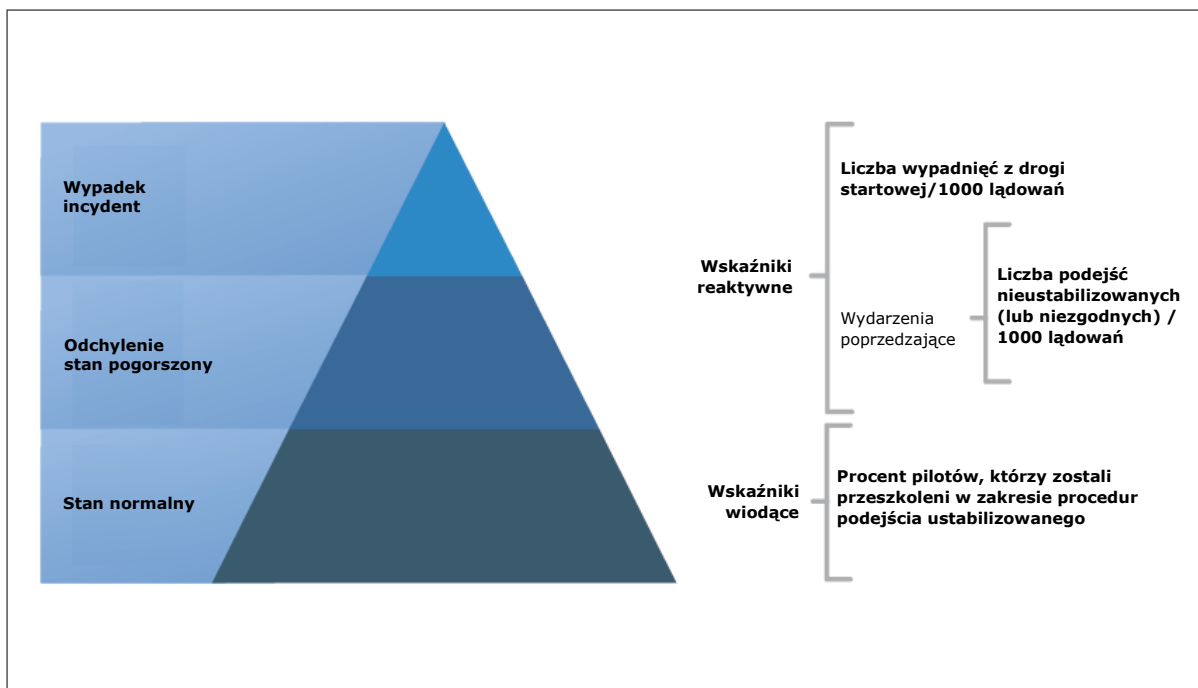


Rysunek 4-2. Koncepcja wskaźników wiodących i reaktywnych

4.3.2.3 SPI powinny być:

- a) związane z celem bezpieczeństwa, który zamierzają wskazać;
- b) wybrane lub opracowane na podstawie dostępnych danych i wiarygodnych pomiarów;
- c) odpowiednio szczegółowe i wymierne; oraz
- d) realistyczne, biorąc pod uwagę możliwości i ograniczenia organizacji.

4.3.2.4 Zazwyczaj wymagana jest kombinacja SPI, aby zapewnić wyraźne wskazanie poziomu bezpieczeństwa. Powinien istnieć wyraźny związek między wskaźnikami reaktywnymi a wiodącymi. Najlepiej gdyby wskaźniki reaktywne były definiowane przed określeniem wskaźników wiodących. Zdefiniowanie wskaźnika prekursorowego powiązanego z poważniejszym zdarzeniem lub stanem (wskaźnik reaktywny) zapewnia wyraźną korelację między tymi dwoma. Wszystkie wskaźniki SPI, zarówno reaktywne jak i wiodące, są równie ważne i wartościowe. Przykład tych powiązań został przedstawiony na Rysunku 4-3.



Rysunek 4-3. Przykłady powiązań pomiędzy wskaźnikami reaktywnymi a wskaźnikami wiodącymi

4.3.2.5 Ważne jest, aby dokonać wyboru wskaźników SPI, które odnoszą się do celów bezpieczeństwa organizacji. Dobrze zdefiniowane i dostosowane wskaźniki SPI ułatwią identyfikację celów poziomów bezpieczeństwa (SPT), co wykaże postęp w osiąganiu celów bezpieczeństwa. Dzięki temu organizacja może przypisać zasoby dla uzyskania jak największego efektu związanego z bezpieczeństwem, poprzez posiadanie dokładnej wiedzy, co jest wymagane, oraz kiedy i jak działać w celu osiągnięcia planowanego poziomu bezpieczeństwa. Na przykład, Państwo ma cel bezpieczeństwa polegający na „zmniejszeniu liczby wypadnięć z drogi startowej o 50 procent w ciągu trzech lat” i powiązany, dobrze dopasowany wskaźnik SPI „liczby wypadnięć z drogi startowej na milion odlotów na wszystkich lotniskach”. Jeżeli liczba wypadnięć spada w fazie początkowej, gdy rozpoczyna się monitorowanie, ale zaczyna ponownie wzrastać po dwunastu miesiącach, Państwo może zdecydować się na realokację zasobów poza obszar, w którym zgodnie z SPI cel bezpieczeństwa jest łatwo osiągalny, w kierunku zmniejszenia liczby wypadnięć z drogi startowej w celu złagodzenia niepożądanego trendu.

Definiowanie SPI

4.3.2.6 W treści każdego SPI należy zawrzeć:

- a) opis elementów, które mierzy SPI;
- b) cel SPI (czym ma na celu zarządzać i kogo ma informować);
- c) jednostki miary i wszelkie wymagania dotyczące jego obliczenia;
- d) kto jest odpowiedzialny za gromadzenie, walidację, monitorowanie, zgłaszanie i realizację działań w oparciu o SPI (mogą to być pracownicy z różnych części organizacji);
- e) gdzie lub w jaki sposób dane powinny być gromadzone; oraz
- f) częstotliwość zgłaszania, gromadzenia, monitorowania i analizy danych SPI.

Wskaźniki SPI i zgłaszanie zdarzeń związanych z bezpieczeństwem

4.3.2.7 Zmiany praktyk operacyjnych mogą prowadzić do niedostatecznego zgłaszania, do momentu kiedy wpływ tych zmian nie zostanie w pełni zaakceptowany przez potencjalne osoby zgłaszające. Jest to tzw.

„stronniczość zgłaszania”. Zmiany w przepisach związanych z ochroną informacji dotyczących bezpieczeństwa i powiązanych źródeł mogą prowadzić do nadmiernego zgłaszania. W obu przypadkach stronniczość zgłaszania może zniekształcić intencję i dokładność danych wykorzystywanych we wskaźniku SPI. Zgłaszanie zdarzeń związanych z bezpieczeństwem, realizowane zdroworozsądkowo, może stanowić źródło cennych danych do zarządzania poziomem bezpieczeństwa.

4.3.3 Wyznaczanie celów poziomów bezpieczeństwa (SPT)

4.3.3.1 Cele poziomów bezpieczeństwa (SPT) określają krótko- i średnioterminowe osiągnięcia pożądane w zakresie zarządzania poziomem bezpieczeństwa. Działają jako „kamienie milowe”, które dają pewność, że organizacja jest na dobrej drodze do osiągnięcia swoich celów w zakresie bezpieczeństwa oraz zapewniają wymierny sposób weryfikacji skuteczności działań związanych z zarządzaniem poziomem bezpieczeństwa. Wyznaczenie SPT powinno uwzględniać takie czynniki jak dominujący poziom ryzyka bezpieczeństwa, tolerowanie ryzyka bezpieczeństwa, a także oczekiwania dotyczące bezpieczeństwa danego sektora lotnictwa. Wyznaczenie SPT powinno być określane po rozważeniu, co jest realnie osiągalne dla powiązanego sektora lotnictwa i uwzględnieniu ostatnich wyników danego wskaźnika SPI, gdzie dostępne są historyczne dane na temat trendów.

4.3.3.2 Jeżeli połączenie celów w zakresie bezpieczeństwa, wskaźników SPI i poziomów SPT współdziałających razem jest konkretne, wymierne, osiągalne, istotne i aktualne (SMART), pozwala to organizacji bardziej skutecznie wykazać swój poziom bezpieczeństwa. Istnieje wiele podejść do osiągnięcia celów zarządzania poziomem bezpieczeństwa, w szczególności poprzez wyznaczenie SPT. Jedno z podejść obejmuje ustanowienie ogólnych celów w zakresie bezpieczeństwa wraz z dostosowanymi wskaźnikami SPI, a następnie określenie rozsądnych poziomów poprawy po ustaleniu bazowego poziomu bezpieczeństwa. Te poziomy poprawy mogą być oparte na konkretnych celach szczegółowych (np. procentowy spadek) lub osiągnięciu pozytywnego trendu. Innym podejściem, które można zastosować, gdy cele w zakresie bezpieczeństwa są SMART, jest zapewnienie, aby cele szczegółowe działały jako kamienie milowe w osiąganiu celów w zakresie bezpieczeństwa. Każde z tych podejść jest ważne i mogą istnieć inne, które organizacja uzna za skuteczne w wykazaniu swojego poziomu bezpieczeństwa. Różne podejścia można stosować w połączeniu stosownie do określonych okoliczności.

Wyznaczanie celów szczegółowych z celami ogólnymi w zakresie bezpieczeństwa

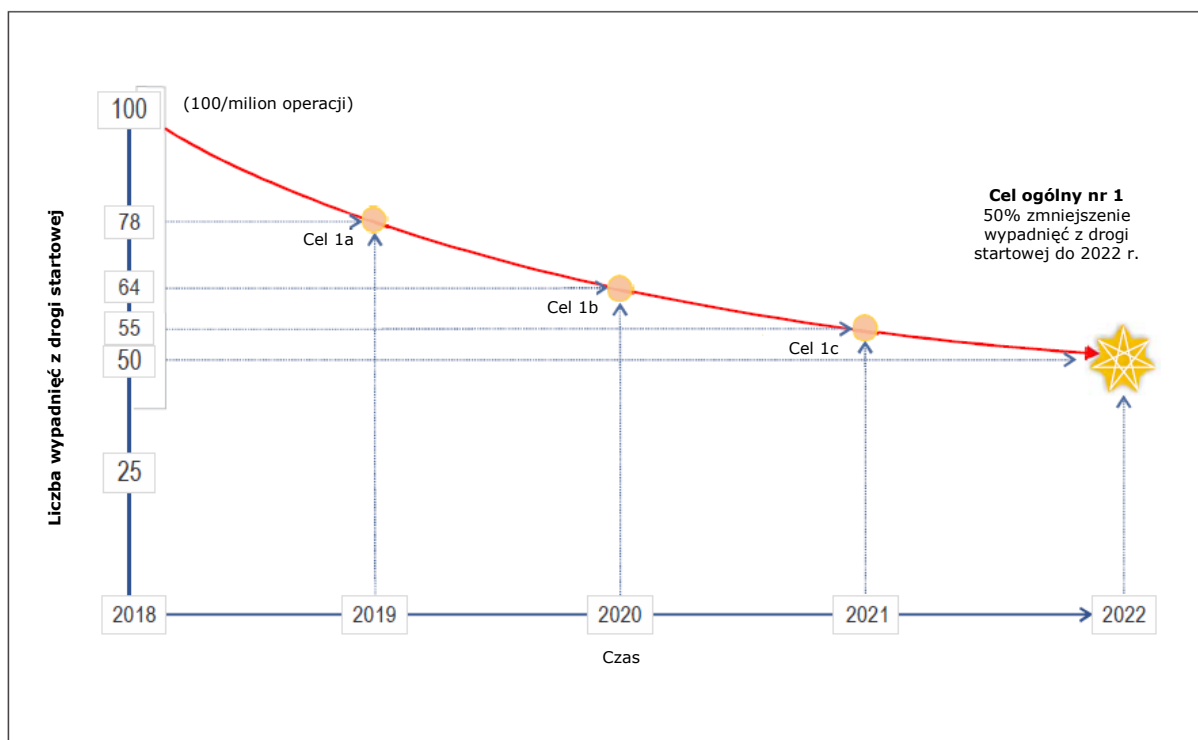
4.3.3.3 Cele szczegółowe są ustanawiane kiedy kierownictwo wyższego szczebla uzgodniło cele ogólne w zakresie bezpieczeństwa. Następnie organizacja identyfikuje odpowiednie wskaźniki SPI, które pokażą poprawę poziomu bezpieczeństwa w kierunku uzgodnionych celów w zakresie bezpieczeństwa. Wskaźniki SPI będą mierzone przy użyciu istniejących źródeł danych, ale mogą również wymagać gromadzenia dodatkowych danych. Następnie organizacja rozpoczyna gromadzenie, analizowanie i prezentowanie wskaźników SPI. Zaczną się pojawiać trendy, które zapewnią obraz poziomu bezpieczeństwa organizacji i czy zmierza on w kierunku celów w zakresie bezpieczeństwa, czy też nie. W tym momencie organizacja może zidentyfikować rozsądne i osiągalne SPT dla każdego wskaźnika SPI.

Wyznaczanie celów szczegółowych z celami w zakresie bezpieczeństwa SMART

4.3.3.4 Cele w zakresie bezpieczeństwa mogą być trudne do przekazania i mogą stanowić wyzwanie do osiągnięcia. Dzieląc je na mniejsze szczegółowe cele bezpieczeństwa, proces ich osiągania jest łatwiejszy. W ten sposób cele szczegółowe stanowią kluczowe ogniwo pomiędzy strategią a codziennymi operacjami. Organizacje powinny zidentyfikować kluczowe obszary, które wpływają na poziom bezpieczeństwa i ustalić sposób ich pomiaru. Kiedy organizacja ma rozeznanie, jaki jest jej obecny poziom poprzez ustalenie bazowego poziomu bezpieczeństwa, może ona rozpocząć określanie SPT, aby dać każdemu w Państwie jednoznaczne odczucie, do czego powinni dążyć. Organizacja może również wykorzystywać analizę porównawczą jako wsparcie przy określaniu celów szczegółowych. Wiąże się to z wykorzystaniem informacji od podobnych organizacji, które już mierzyły swoją wydajność, aby uzyskać wiedzę jak inni sobie radzą w tym zakresie.

4.3.3.5 Przykład powiązań pomiędzy celami bezpieczeństwa, SPI i SPT przedstawiono na Rysunku 4-4. W tym przykładzie organizacja odnotowała 100 wypadnięć z drogi startowej na milion operacji w 2018 r. Ustalono, że jest to zbyt wiele, i ustalono cel polegający na zmniejszeniu liczby wypadnięć z drogi startowej o 50% do 2022 r. Określono ukierunkowane działania i powiązane ramy czasowe dla osiągnięcia tych szczegółowych celów. Aby monitorować, mierzyć i zgłaszać swoje postępy, organizacja wybrała jako wskaźnik SPI „wypadnięcia z drogi startowej na milion operacji rocznie”. Organizacja jest świadoma, że postęp będzie szybszy i skuteczniejszy, jeżeli określone zostaną konkretne cele, które są zgodne z celem bezpieczeństwa. W związku z tym ustalono cel bezpieczeństwa, który odpowiada średniej redukcji o 12,5% rocznie w danym okresie sprawozdawczym (cztery lata). Jak pokazano w formie graficznej, oczekuje się, że postęp będzie większy w pierwszych latach, a mniejszy w późniejszych latach. Zostało to przedstawione przez krzywą biegnącą w kierunku celu. Na Rysunku 4-4:

- a) celem w zakresie bezpieczeństwa SMART jest „50-procentowe zmniejszenie wskaźnika wypadnięć z drogi startowej do 2022 r.”;
- b) wybrany wskaźnik SPI to „liczba wypadnięć z drogi startowej na milion operacji rocznie”; oraz
- c) szczegółowe cele bezpieczeństwa związane z tym celem stanowią kamienie milowe dla osiągnięcia celu bezpieczeństwa SMART i są równe ~12,5% zmniejszenia rocznie do 2022 r. ;
 - 1) SPT 1a wynosi „mniej niż 78 wypadnięć z drogi startowej na milion operacji w 2019 r.”;
 - 2) SPT 1b wynosi „mniej niż 64 wypadnięcia z drogi startowej na milion operacji w 2020 r.”;
 - 3) SPT 1c wynosi „mniej niż 55 wypadnięć z drogi startowej na milion operacji w 2021 r.”.



Rysunek 4-4. Przykłady SPT z celami bezpieczeństwa SMART

Dodatkowe uwarunkowania dotyczące wyboru SPI i SPT

4.3.3.6 Przy wyborze SPI i SPT należy również wziąć pod uwagę:

- a) *Zarządzanie obciążeniem pracą.* Stworzenie wykonalnej ilości wskaźników SPI może pomóc personelowi w ich monitorowaniu i zapobiec nadmiernemu obciążeniu związanemu ze zgłaszaniem. To samo dotyczy złożoności wskaźników SPI lub dostępności niezbędnych danych. Lepiej jest uzgodnić, co jest wykonalne, a następnie, na tej podstawie, ustalić priorytety dotyczące wyboru wskaźników SPI. Jeżeli SPI nie stanowi źródła informacji o poziomie bezpieczeństwa lub otrzymał niższy priorytet, należy rozważyć zaprzestanie jego stosowania na rzecz wskaźnika bardziej użytecznego lub posiadającego wyższy priorytet.
- b) *Optymalny rozkład wskaźników SPI.* Kombinacja wskaźników SPI obejmująca obszary największego zainteresowania pomoże uzyskać wgląd w ogólny poziom bezpieczeństwa organizacji i umożliwi podejmowanie decyzji w oparciu o dane.
- c) *Klarowność wskaźników SPI.* Przy wyborze SPI należy mieć jasność co do przedmiotu i częstotliwości pomiaru. Wskaźniki SPI posiadające jasne definicje pomagają w zrozumieniu wyników, unikaniu błędów w interpretacji i pozwalają na sensowne porównania w czasie.
- d) *Zachęcanie do pożądanego zachowania.* SPT mogą wpływać na zmianę zachowania i przyczynić się do pożądanego wyniku. Jest to szczególnie istotne, jeżeli osiągnięcie celu końcowego wiąże się z nagrodami organizacyjnymi, takimi jak wynagrodzenie za zarządzanie. SPT powinny sprzyjać pozytywnym zachowaniom organizacyjnym i indywidualnym, które w sposób zamierzony prowadzą do uzasadnionych decyzji i poprawy poziomu bezpieczeństwa. Przy wyborze SPI i SPT równie ważne jest uwzględnienie potencjalnie niezamierzonych zachowań.
- e) *Wybór wartościowych obszarów pomiaru.* Konieczne jest wybranie przydatnych wskaźników SPI, a nie tylko tych łatwych do zmierzenia. Organizacja powinna zdecydować, jakie są najbardziej przydatne parametry bezpieczeństwa, które prowadzą organizację w kierunku poprawy w podejmowaniu decyzji, zarządzaniu poziomem bezpieczeństwa i osiągnięciu celów bezpieczeństwa.
- f) *Osiąganie SPT.* Jest to szczególnie ważne zagadnienie związane z pożądanymi zachowaniami związanymi z bezpieczeństwem. Osiągnięcie uzgodnionych SPT nie zawsze wskazuje na poprawę poziomu bezpieczeństwa. Organizacja powinna rozróżnić pomiędzy osiągnięciem SPT a rzeczywistością, możliwą do wykazania poprawą poziomu bezpieczeństwa organizacji. Konieczne jest, aby organizacja rozważyła kontekst, w którym poziom docelowy został osiągnięty, zamiast rozpatrywać SPT w izolacji. Rozpatrywanie ogólnej poprawy poziomu bezpieczeństwa, zamiast uzyskiwania indywidualnego SPT, będzie sprzyjać pożądanym zachowaniom organizacyjnym i zachęcać do wymiany informacji dotyczących bezpieczeństwa, co stanowi sedno zarówno zarządzania ryzykiem bezpieczeństwa jak również zapewniania bezpieczeństwa. Może to również wzmocnić relacje pomiędzy Państwem a podmiotem lotniczym oraz ich chęć dzielenia się danymi i pomysłami dotyczącymi bezpieczeństwa.

Uwagi dotyczące określenia SPT

4.3.3.7 Definiowanie SPT nie zawsze jest konieczne lub właściwe, ponieważ mogą występować pewne wskaźniki SPI, które lepiej monitorują trendy, aniżeli określają wartość docelową. Zgłaszanie zdarzeń związanych z bezpieczeństwem jest przykładem, kiedy posiadanie celu może zniechęcić ludzi do niezgłaszania (jeżeli celem nie jest przekroczenie liczby) lub zgłaszania trywialnych spraw, aby osiągnąć cel (jeżeli celem jest osiągnięcie określonej liczby). Mogą również być wskaźniki SPI, które są lepiej wykorzystywane do zdefiniowania kierunku działań w celu ciągłej poprawy poziomu bezpieczeństwa (tj. zmniejszenia liczby zdarzeń), a nie do określenia celu

bezwzględny, ponieważ mogą one być trudne do określenia. Przy podejmowaniu decyzji o odpowiednich SPT należy również wziąć pod uwagę następujące kwestie:

- a) Panowanie nad niepożądanymi zachowaniami; jeżeli menedżerowie lub organizacje nadmiernie koncentrują się na osiągnięciu liczb będących wskaźnikiem sukcesu, mogą nie osiągnąć zamierzonej poprawy poziomu bezpieczeństwa.
- b) Cele operacyjne; zbyt duży nacisk na osiąganie celów operacyjnych (takich jak: terminowe odloty, zmniejszenie kosztów ogólnych, itp.) bez zrównoważenia SPT może prowadzić do „osiągnięcia celów operacyjnych”, niekoniecznie poprawiając poziom bezpieczeństwa.
- c) Koncentracja na ilości, a nie jakości; może to zachęcić personel lub wydziały do osiągnięcia celu, przy jednoczesnym zapewnieniu słabego produktu lub usługi.
- d) Innowacje Cap; chociaż nie jest to zamierzone, po osiągnięciu celu może dojść do odprężenia i stwierdzenia, że nie są potrzebne dalsze ulepszenia, oraz może dojść do sytuacji ogólnego samozadowolenia.
- e) Konflikt organizacyjny; cele mogą powodować konflikty pomiędzy wydziałami i organizacjami, ponieważ dochodzi do kłótni o to, kto ponosi odpowiedzialność, zamiast skupić się na próbie współpracy.

4.3.4 Pomiar poziomu bezpieczeństwa

Uzyskanie prawidłowego pomiaru poziomu bezpieczeństwa wymaga podjęcia decyzji, jak najlepiej zmierzyć osiągnięcie celów bezpieczeństwa. Będzie się to różnić w zależności od poszczególnych Państw i podmiotów prowadzących działalność w lotnictwie cywilnym. Organizacje powinny poświęcić czas, aby rozwinąć swoją strategiczną świadomość tego, co napędza poprawę bezpieczeństwa dla celów bezpieczeństwa.

4.3.5 Korzystanie z SPI i SPT

SPI i SPT można wykorzystywać na różne sposoby, aby zademonstrować poziom bezpieczeństwa. Bardzo ważne jest, aby organizacje dostosowywały, wybierały i stosowały różne narzędzia pomiarowe i podejścia w zależności od swoich specyficznych okoliczności i charakteru tego, co jest mierzone. Na przykład w niektórych przypadkach organizacje mogą przyjąć wskaźniki SPI, spośród których wszystkie posiadają konkretne powiązane SPT. W innej sytuacji, lepsze może okazać się skupienie na osiągnięciu pozytywnego trendu we wskaźnikach SPI, bez określonych wartości docelowych. Pakiet wybranych wskaźników działania zazwyczaj będzie wykorzystywał kombinację tych podejść.

4.4. MONITOROWANIE POZIOMU BEZPIECZEŃSTWA

4.4.1 Kiedy organizacja zidentyfikuje cele w oparciu o wskaźniki SPI, które w ich opinii zapewnią planowany wynik, należy zagwarantować, że zainteresowane strony będą postępować zgodnie z jasno określonym przydziałem obowiązków związanym z zapewnieniem wyniku. Zdefiniowanie SPT w przypadku każdej władzy lotniczej, sektora i podmiotu lotniczego wspiera osiągnięcie akceptowalnego poziomu bezpieczeństwa (ALoSP) przez Państwo poprzez jednoznaczne przypisanie odpowiedzialności.

4.4.2 Należy ustanowić mechanizmy monitorowania i pomiaru poziomu bezpieczeństwa organizacji w celu zidentyfikowania zmian, które mogą być potrzebne jeżeli poczynione postępy nie są zgodne z oczekiwaniami, oraz w celu wzmocnienia zaangażowania organizacji w osiągnięcie celów bezpieczeństwa.

4.4.3 Bazowy poziom bezpieczeństwa

Zrozumienie sposobu, w jaki organizacja planuje postęp w realizacji celów bezpieczeństwa, wymaga wiedzy gdzie organizacja znajduje się w odniesieniu do bezpieczeństwa. Jeżeli struktura poziomu bezpieczeństwa organizacji (cele bezpieczeństwa, wskaźniki, wartości docelowe, czynniki uruchamiające) została ustanowiona i funkcjonuje, możliwe jest poznanie bazowego poziomu bezpieczeństwa dla danego okresu monitorowania. Bazowy poziom bezpieczeństwa to poziom bezpieczeństwa w momencie rozpoczęcia procesu pomiaru poziomu bezpieczeństwa, punkt odniesienia, od którego można mierzyć postęp. W przykładzie użytym na Rysunkach 4-3 i 4-4, bazowy poziom bezpieczeństwa dla tego konkretnego celu bezpieczeństwa to „100 wypadnięć z drogi startowej na milion operacji w roku (2018)”. W oparciu o tą solidną podstawę, można rejestrować dokładne i znaczące wskazania i cele.

4.4.4 Udoskonalenie wskaźników SPI i poziomów SPT

4.4.4.1 Wskaźniki SPI i powiązane poziomy SPT będą musiały zostać poddane przeglądowi w celu określenia, czy dostarczają informacji potrzebnych do śledzenia postępów w osiągnięciu celów bezpieczeństwa oraz w celu zapewnienia, że cele są realistyczne i osiągalne.

4.4.4.2 Zarządzanie poziomem bezpieczeństwa jest działaniem ciągłym. Ryzyka bezpieczeństwa i/lub dostępność danych zmieniają się z upływem czasu. Wstępne wskaźniki SPI mogą być opracowywane przy użyciu ograniczonych źródeł informacji dotyczących bezpieczeństwa. Na późniejszym etapie, można ustanowić więcej kanałów zgłaszania, udostępnić więcej danych dotyczących bezpieczeństwa, a możliwości prowadzenia analiz bezpieczeństwa przez organizację będą prawdopodobnie znacznie większe. Początkowo, dla organizacji bardziej odpowiednie może być opracowanie prostych (szerszych) wskaźników SPI. W miarę gromadzenia większej ilości danych i rozwoju możliwości zarządzania bezpieczeństwem, mogą one rozważyć udoskonalenie zakresu SPI i SPT w celu lepszego dostosowania do pożądaných celów bezpieczeństwa. Małe, niezłożone organizacje mogą zdecydować się na udoskonalenie SPI i SPT i/lub wybrać ogólne (ale konkretne) wskaźniki, które mają zastosowanie do większości systemów lotniczych. Niektóre przykłady ogólnych wskaźników to:

- a) zdarzenia, w tym uszkodzenia strukturalne sprzętu;
- b) zdarzenia wskazujące okoliczności, w których wypadek prawie wystąpił;
- c) zdarzenia, w których personel operacyjny lub członkowie społeczności lotniczej byli śmiertelnie lub poważnie ranni;
- d) zdarzenia, w których personel operacyjny stał się ubezwłasnowolniony lub niezdolny do bezpiecznego wykonywania swoich obowiązków;
- e) wskaźnik dobrowolnych zgłoszeń zdarzeń; oraz
- f) wskaźnik obowiązkowych zgłoszeń zdarzeń.

4.4.4.3 Większe, bardziej złożone organizacje mogą zdecydować się na wprowadzenie szerszego i/lub dokładniejszego zakresu SPI i SPT oraz zintegrowanie wskaźników ogólnych, takich jak te wymienione powyżej, ze wskaźnikami specyficznymi dla prowadzonej działalności. Duże lotnisko, na przykład, świadczące usługi dla dużych linii lotniczych i znajdujące się w skomplikowanej przestrzeni powietrznej, może rozważyć połączenie niektórych ogólnych wskaźników SPI z dokładniejszymi wskaźnikami SPI reprezentującymi określone aspekty działania. Monitorowanie takich wskaźników może wymagać większego wysiłku, ale prawdopodobnie przyniesie lepsze wyniki w zakresie bezpieczeństwa. Istnieje wyraźna korelacja pomiędzy względną złożonością SPI i SPT a skalą i złożonością operacji prowadzonych przez Państwo lub podmioty lotnicze. Ta względna złożoność powinna znaleźć odzwierciedlenie w zestawie wskaźników i celów. Osoby odpowiedzialne za zarządzanie poziomem bezpieczeństwa powinny być tego świadome.

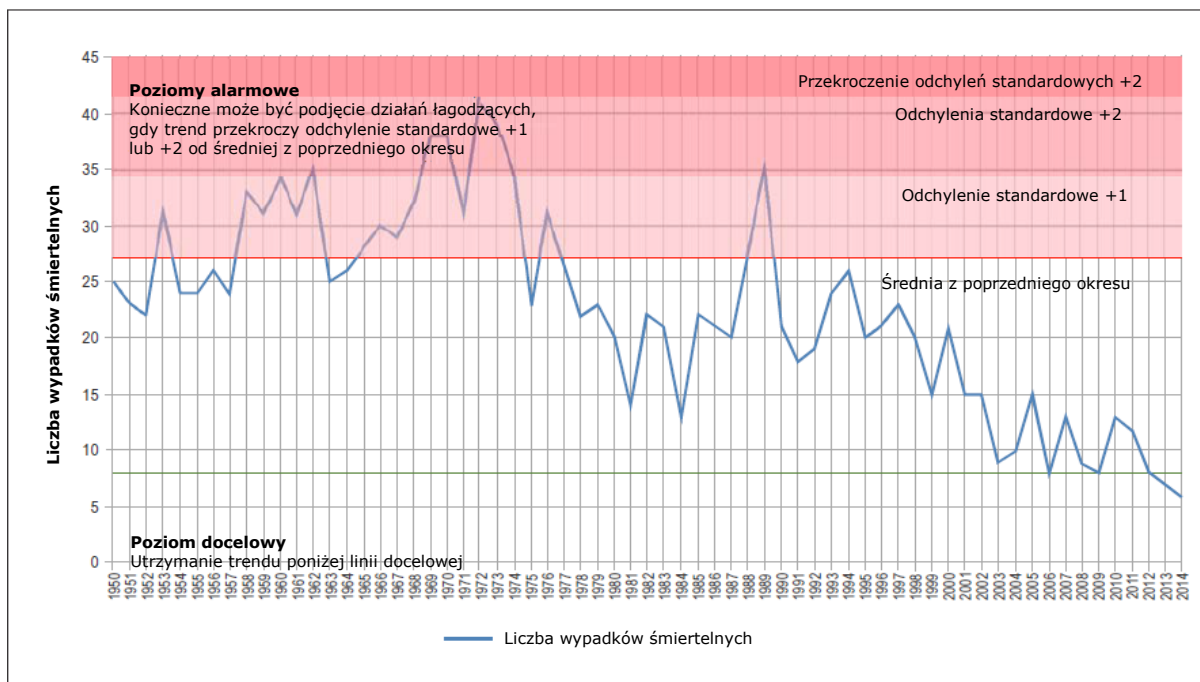
4.4.4.4 Zestaw SPI i SPT wybranych przez organizację powinien być poddawany okresowym przeglądom, aby zapewnić ich ciągłą zasadność jako wskaźnik poziomu bezpieczeństwa organizacji. Oto niektóre powody, aby kontynuować, przerwać lub zmienić SPI i SPT:

- a) wskaźniki SPI stale przedstawiają tę samą wartość (np. zero procent lub 100 procent); jest mało prawdopodobne, że zapewnią one istotny wkład w podejmowanie decyzji przez kierownictwo wyższego szczebla;
- b) wskaźniki SPI, które wykazują się podobnym zachowaniem i jako takie są uważane za powielenie;
- c) osiągnięty został SPT dla wskaźnika SPI wdrożonego w celu pomiaru wdrożenia programu lub ukierunkowanej poprawy;
- d) inny problem dotyczący bezpieczeństwa staje się priorytetem i wymaga monitorowania i pomiaru;
- e) aby lepiej zrozumieć konkretny problem dotyczący bezpieczeństwa poprzez zawężenie specyfiki wskaźnika SPI (tj. zmniejszyć „szum”, aby oczyścić „sygnał”); oraz
- f) cele bezpieczeństwa uległy zmianie i w konsekwencji wskaźniki SPI wymagają aktualizacji, aby pozostały odpowiednie.

4.4.5 Czynniki uruchamiające bezpieczeństwo

4.4.5.1 Krótkie odniesienie do pojęcia czynników uruchamiających jest istotne, aby wskazać ich ewentualną rolę w kontekście zarządzania poziomem bezpieczeństwem przez organizację.

4.4.5.2 Czynnikiem uruchamiającym jest ustalona wartość poziomu lub kryterium, która służy do uruchomienia (rozpoczęcia) oceny, decyzji, dostosowania lub działania naprawczego związanego z danym wskaźnikiem. Jedną z metod ustawiania kryteriów aktywacji poza limitami dla SPT jest zastosowanie zasady odchylenia standardowego w populacji (STDEVP). Metoda ta wywodzi wartość odchylenia standardowego (SD) w oparciu o poprzednie historyczne punkty danych danego wskaźnika bezpieczeństwa. Wartość odchylenia standardowego plus przeciętna (średnia) wartość zestawu danych historycznych stanowi podstawową wartość uruchamiającą dla następnego okresu monitorowania. Zasada odchylenia standardowego (podstawowa funkcja statystyczna) określa kryteria poziomu uruchamiającego na podstawie rzeczywistych wyników historycznych dla danego wskaźnika (zestawu danych), w tym jego zmienności (wahania punktów danych). Bardziej zmienny zestaw danych historycznych zazwyczaj powoduje wyższą wartość poziomu uruchamiającego dla następnego okresu monitorowania. Czynniki uruchamiające zapewniają wczesne ostrzeżenia, które umożliwiają decydom podejmowanie świadomych decyzji dotyczących bezpieczeństwa, a tym samym poprawiają poziom bezpieczeństwa. Przykład poziomów uruchamiających na podstawie odchyleń standardowych (SD) został przedstawiony na Rysunku 4-5 poniżej. W przykładzie tym, podjęcie decyzji w oparciu o dane oraz działań łagodzących może być konieczne, kiedy trend przekroczy wartość + 1SD lub + 2SD od średniej z poprzedniego okresu. Często poziomy uruchamiający (w tym przypadku + 1SD, + 2SD lub poza + 2SD) będą zgodne z poziomami zarządzania decyzjami i stopniem pilności działania.



Rysunek 4-5. Przykład zobrazowania poziomów uruchamiających (alarmowych) bezpieczeństwa

4.4.5.3 Po zdefiniowaniu SPT i ustawień czynników uruchamiających (jeżeli są używane), powiązane z nimi wskaźniki SPI mogą być śledzone pod kątem statusu ich działania. Skonsolidowane podsumowanie ogólnego wyniku działania SPT i czynnika uruchamiającego całego pakietu wskaźników SPI może być również skompilowane i/lub zagregowane dla danego okresu monitorowania. Wartości jakościowe (dostateczne/niedostateczne) mogą być przypisane dla każdego przypadku osiągnięcia SPT, i każdego poziomu aktywacji, który nie został naruszony. Alternatywnie, wartości liczbowe (punkty) mogą być użyte do zapewnienia ilościowego pomiaru ogólnego działania pakietu wskaźników SPI.

4.4.5.4 Należy zauważyć, że wartości czynników uruchamiających służą do aktywowania (rozpoczęcia) oceny, decyzji, dostosowania lub działania naprawczego związanego z danym wskaźnikiem. Aktywowany wskaźnik SPI niekoniecznie musi być katastrofalny lub wskazywać na awarię. Jest to tylko znak, że działanie przekroczyło ustalony limit. Czynniki uruchamiające ma na celu zwrócenie uwagi decydentów, którzy mogą podjąć działania naprawcze, lub nie, w zależności od okoliczności.

4.4.6 Uwagi dotyczące czynników uruchamiających

4.4.6.1 Istnieją wyzwania związane z określeniem wiarygodnych poziomów dla czynników uruchamiających. Czynniki uruchamiające i związane z nimi poziomy działają najlepiej, gdy istnieją obszernie dane bezpieczeństwa i możliwości ich zarządzania. Może to nałożyć dodatkowe obciążenie na organizację. Pojęcie uruchomienia zostało zaprojektowane i najlepiej pasuje do zarządzania ryzykiem bezpieczeństwa w odniesieniu do systemów czysto technicznych (np. monitorowanie silników lotniczych). W tym przypadku, duże ilości danych ilościowych zapewniają wsparcie w identyfikacji dokładnych czynników uruchamiających i ich poziomów. Pojęcie czynników uruchamiających jest prawdopodobnie mniej istotne dla zarządzania ryzykiem bezpieczeństwa w odniesieniu do systemów społeczno-technicznych. Systemy społeczno-techniczne to systemy, w których ludzie aktywnie współdziałają z procesami i technologiami w celu zapewnienia usługi oraz osiągnięcia celów produkcyjnych systemu. Zarówno krajowy program bezpieczeństwa jak i system zarządzania bezpieczeństwem stanowią systemy społeczno-techniczne. Mniej wiarygodne i znaczące czynniki uruchamiające stosowane w systemach społeczno-technicznych wynikają z ograniczeń niezawodnych środków, w które zaangażowani są ludzie.

4.4.6.2 Potrzebne jest zatem bardziej elastyczne podejście, aby czynniki uruchamiające miały sens. Załącznik 19 nie wymaga, aby Państwa lub podmioty lotnicze określały poziomy uruchamiające dla każdego

wskaźnika SPI. Istnieją jednak korzyści dla organizacji, w których dane dla wskaźnika SPI są bardzo konkretne, istnieje wystarczająco dużo punktów danych, a dane są dostatecznie wiarygodne.

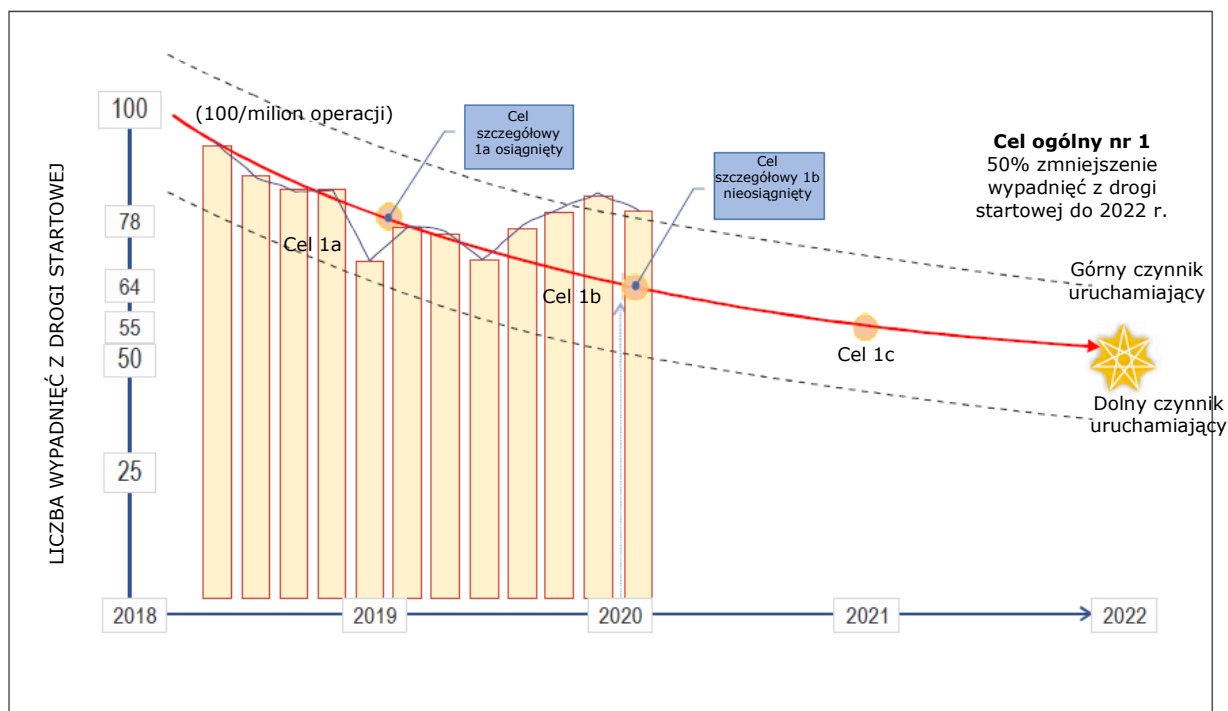
4.4.6.3 Rysunek 4-6 poniżej stanowi rozszerzenie poprzedniego przykładu, „50-procentowego zmniejszenia wypadnięć z drogi startowej do roku 2022”. W scenariuszu tym jest teraz rok 2020. Organizacja zbierała dane bezpieczeństwa (SPI - „Brak wypadnięć z drogi startowej/milion operacji/rok”) i współpracowała z zainteresowanymi stronami w celu zmniejszenia liczby takich przypadków. SPT na rok 2019 (<78 wypadnięć z drogi startowej/milion operacji rocznie) został osiągnięty. Wskaźnik SPI pokazuje jednak, że nie tylko SPT za rok 2020 (<64 wypadnięcia z drogi startowej/milion operacji rocznie) nie został osiągnięty, liczba wypadnięć przekroczyła czynnik uruchamiający w dwóch kolejnych okresach sprawozdawczych. Decydenci zostali powiadomieni o pogorszeniu poziomu bezpieczeństwa i są w stanie podejmować decyzje na podstawie danych w celu podjęcia dalszych działań. Ich decyzje oparte na danych będą zmierzać do przywrócenia poziomu bezpieczeństwa z powrotem do akceptowalnego zakresu, i są na drodze do osiągnięcia ich celu bezpieczeństwa.

4.4.7 Identyfikacja wymaganych działań

4.4.7.1 Prawdopodobnie najważniejszym wynikiem ustanowienia struktury zarządzania poziomem bezpieczeństwa jest zapewnienie informacji decydentom organizacji w taki sposób, aby mogli oni podejmować decyzje na podstawie aktualnych i wiarygodnych danych dotyczących bezpieczeństwa i informacji dotyczących bezpieczeństwa. Celem powinno być zawsze podejmowanie decyzji zgodnie z polityką bezpieczeństwa i celami bezpieczeństwa.

4.4.7.2 W odniesieniu do zarządzania poziomem bezpieczeństwa, podejmowanie decyzji w oparciu o dane polega na podejmowaniu skutecznych, świadomych decyzji opartych na wynikach monitorowanych i mierzonych wskaźników SPI lub na innych raportach i analizie danych bezpieczeństwa i informacji bezpieczeństwa. Korzystanie z ważnych i istotnych danych bezpieczeństwa w połączeniu z informacjami zapewniającymi kontekst wspiera organizację w podejmowaniu decyzji zgodnych z celami bezpieczeństwa. Informacje kontekstowe mogą również obejmować inne priorytety zainteresowanych stron, znane braki w danych i inne uzupełniające dane do oceny zalet, wad, możliwości, ograniczeń i ryzyk w odniesieniu do decyzji jaka ma być podjęta. Posiadanie informacji łatwo dostępnych i łatwych do interpretacji pomaga złagodzić stronniczość, wpływy i błędy ludzkie w procesie podejmowania decyzji.

4.4.7.3 Podejmowanie decyzji w oparciu o dane wspiera również ocenę decyzji podjętych w przeszłości w celu zapewnienia wsparcia w dostosowaniu do celów bezpieczeństwa. Więcej wytycznych dotyczących podejmowania decyzji w oparciu o dane znajduje się w Rozdziale 6.



Rysunek 4-6. Przykład ustawienia czynników uruchamiających

4.5. AKTUALIZACJA CELÓW BEZPIECZEŃSTWA

W zarządzaniu poziomem bezpieczeństwa nie ma zastosowania podejście typu „ustalić i zapomnieć”. Zarządzanie poziomem bezpieczeństwa ma charakter dynamiczny i ma kluczowe znaczenie dla funkcjonowania każdego Państwa i każdego podmiotu prowadzącego działalność w lotnictwie cywilnym, i powinno być poddawane przeglądowi i aktualizacji:

- rutynowo, zgodnie z cyklem okresowym ustalonym i uzgodnionym przez komisję ds. bezpieczeństwo wysokiego szczebla;
- w oparciu o dane wejściowe z analiz bezpieczeństwa (szczegółowe informacje znajdują się w Rozdziale 6); oraz
- w odpowiedzi na poważne zmiany w działaniu, najwyższe ryzyka lub środowisko.

ROZDZIAŁ 5

SYSTEMY ZBIERANIA I PRZETWARZANIA DANYCH BEZPIECZEŃSTWA

5.1. WSTĘP

5.1.1 Rozróżnienie pomiędzy danymi bezpieczeństwa a informacjami bezpieczeństwa dokonane zostało w definicjach zawartych w Załączniku 19. Dane bezpieczeństwa są początkowo zgłaszane lub rejestrowane w wyniku obserwacji lub pomiaru. Są one przetwarzane na informacje bezpieczeństwa, kiedy są przetwarzane, organizowane, integrowane lub analizowane w danym kontekście, aby były przydatne do zarządzania bezpieczeństwem. Informacje bezpieczeństwa mogą być nadal przetwarzane na różne sposoby, aby uzyskać różne znaczenia.

5.1.2 Skuteczne zarządzanie bezpieczeństwem zależy w dużym stopniu od skuteczności gromadzenia danych bezpieczeństwa, analizy i ogólnych możliwości zarządzania. Posiadanie solidnych podstaw w postaci danych bezpieczeństwa i informacji bezpieczeństwa ma zasadnicze znaczenie dla zarządzania bezpieczeństwem, ponieważ stanowi bazę do podejmowania decyzji w oparciu o dane. Niezawodne dane bezpieczeństwa i informacje bezpieczeństwa są potrzebne do identyfikacji trendów, podejmowania decyzji i oceny poziomu bezpieczeństwa w odniesieniu do szczegółowych celów bezpieczeństwa i celów w zakresie bezpieczeństwa oraz do oceny ryzyka.

5.1.3 Załącznik 19 wymaga, aby podmioty lotnicze opracowały i utrzymywały formalny proces zbierania, rejestrowania, obsługiwania i generowania informacji zwrotnych na temat zagrożeń w swoich działaniach, w oparciu o połączenie reaktywnych i proaktywnych metod gromadzenia danych dotyczących bezpieczeństwa.

5.1.4 Podobnie Rozdział 8 Załącznika 13 – *Badanie wypadków i incydentów lotniczych* wymaga od Państw ustanowienia i utrzymywania bazy danych wypadków i incydentów w celu ułatwienia skutecznej analizy informacji o faktycznych lub potencjalnych brakach w zakresie bezpieczeństwa oraz określenia wymaganych działań zapobiegawczych.

5.1.5 Załącznik 19 wymaga od Państw ustanowienia systemów zbierania i przetwarzania danych bezpieczeństwa (SDCPS) w celu gromadzenia, przechowywania, agregowania i umożliwienia analizy danych bezpieczeństwa i informacji bezpieczeństwa w celu wsparcia działań związanych z zarządzaniem poziomem bezpieczeństwa. SDCPS to ogólny termin odnoszący się do systemów przetwarzania i zgłaszania, baz danych i schematów wymiany informacji bezpieczeństwa i zapisanych informacji. Termin „baza danych dotyczących bezpieczeństwa” może odnosić się do pojedynczej lub wielu baz danych. Władze Państwa odpowiedzialne za wdrożenie SSP powinny mieć dostęp do SDCPS w celu zapewnienia wsparcia w realizacji ich obowiązków w zakresie bezpieczeństwa.

5.1.6 Podmioty lotnicze są również zobowiązane do opracowania i utrzymania środków służących weryfikacji ich poziomu bezpieczeństwa w odniesieniu do SPI i SPT, w celu wsparcia ich celów w zakresie bezpieczeństwa za pomocą systemu SDCPS. Środki te mogą być oparte na reaktywnych i proaktywnych metodach gromadzenia danych dotyczących bezpieczeństwa i informacji dotyczących bezpieczeństwa.

5.1.7 Wytyczne zawarte w niniejszym rozdziale są równie ważne dla Państw jak i dla podmiotów lotniczych w celu zapewnienia, że zebrane dane bezpieczeństwa i informacje bezpieczeństwa umożliwią skuteczne i prawidłowe podejmowanie decyzji.

5.1.8 Organizacje powinny upewnić się, że posiadają wykwalifikowany personel do zbierania i przechowywania danych bezpieczeństwa oraz posiadający kompetencje potrzebne do przetwarzania danych bezpieczeństwa. Zwykle wymaga to osób o dużych umiejętnościach w zakresie technologii informatycznych, a także posiadających

wiedzę na temat wymagań dotyczących danych, standaryzacji danych, gromadzenia i przechowywania danych, zarządzania danymi i umiejętność rozumienia potencjalnych zapytań, które mogą być potrzebne do analizy. Ponadto organizacja powinna zapewnić, że każdy system SDCPS posiada wyznaczoną osobę, który zapewnia ochronę danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł w zgodzie z Dodatkiem 3 do Załącznika 19. Rozdział 7 zawiera dalsze szczegółowe informacje.

5.2. ZBIERANIE DANYCH BEZPIECZEŃSTWA I INFORMACJI BEZPIECZEŃSTWA

5.2.1 Cele na różnych poziomach systemu lotniczego

5.2.1.1 Poczynając od lat siedemdziesiątych ICAO wprowadza przepisy w postaci Załączników, Procedur służb żeglugi powietrznej (PANS) i dokumentów, które wymagają od Państw ustanowienia systemów zgłaszania w celu gromadzenia danych bezpieczeństwa i informacji bezpieczeństwa. Większość tych przepisów odnosi się do sektorowych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa, z wyjątkiem Załącznika 13, który koncentruje się w szczególności na zgłaszaniu wypadków i poważnych incydentów. Przepisy dotyczące obowiązkowych i dobrowolnych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa, znajdujące się w Załączniku 19, mają swoje źródło w Załączniku 13.

5.2.1.2 Wiele podmiotów lotniczych zgromadziło dużą ilość danych bezpieczeństwa i informacji bezpieczeństwa, w tym w ramach obowiązkowego i dobrowolnego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa, jak również w ramach zautomatyzowanych systemów zbierania danych. Te dane bezpieczeństwa i informacje bezpieczeństwa pozwalają podmiotom prowadzącym działalność w lotnictwie cywilnym na identyfikację zagrożeń i wspieranie działań związanych z zarządzaniem poziomem bezpieczeństwa na poziomie podmiotu. Udostępnianie informacji bezpieczeństwa wiąże się z wieloma korzyściami, w tym z identyfikacją zagrożeń wykraczających poza zasięg pojedynczego podmiotu. Informacje na temat udostępniania i wymiany informacji dotyczących bezpieczeństwa znajdują się w Rozdziale 6.

5.2.1.3 Załącznik 19 wymaga od państw ustanowienia systemu SDCPS w celu zbierania, przechowywania, agregowania i umożliwienia analizy danych bezpieczeństwa i informacji bezpieczeństwa w celu wsparcia identyfikacji zagrożeń, które występują w całym systemie lotniczym. Oznacza to coś więcej niż tylko dostęp w postaci podglądu danych w celu monitorowania poziomu bezpieczeństwa podmiotów lotniczych. Ponadto, wprowadzenie systemów zgłaszania i baz danych do zbierania danych bezpieczeństwa i informacji bezpieczeństwa nie jest wystarczające, aby zapewnić dostępność danych bezpieczeństwa do prowadzenia analizy. Państwa muszą również wprowadzić przepisy, regulacje, procesy i procedury, aby upewnić się, że dane bezpieczeństwa i informacje bezpieczeństwa określone w Załączniku 19 są zgłaszane i zbierane od podmiotów lotniczych i innych jednostek w celu zasilania systemu SDCPS. Wymaga to posiadania środków ochrony zgodnie z Załącznikiem 19, Dodatek 3, w celu zapewnienia wykorzystania danych bezpieczeństwa i informacji bezpieczeństwa na potrzeby utrzymania lub poprawy bezpieczeństwa. Możliwe jest również dokonanie ustaleń ze stroną trzecią, która w imieniu Państwa będzie zbierać, przechowywać i analizować dane bezpieczeństwa i informacje bezpieczeństwa. Informacje na temat ochrony danych bezpieczeństwa i informacji bezpieczeństwa znajdują się w Rozdziale 7.

5.2.1.4 Ponadto dane bezpieczeństwa i informacje bezpieczeństwa muszą być zbierane, przechowywane i analizowane na poziomie regionalnym za pośrednictwem regionalnych grup ds. bezpieczeństwa lotniczego (RASG) w celu ułatwienia identyfikacji zagrożeń wykraczających poza granice Państw oraz promowania wspólnych wysiłków na rzecz łagodzenia ryzyk bezpieczeństwa.

5.2.2 Określanie, co należy zbierać

5.2.2.1 Każda organizacja musi określić, jakie dane bezpieczeństwa i informacje bezpieczeństwa musi zebrać w celu wsparcia procesu zarządzania poziomem bezpieczeństwa oraz podejmowania decyzji dotyczących bezpieczeństwa. Wymogi dotyczące danych i informacji bezpieczeństwa można określić przy użyciu podejścia odgórnego i/lub oddolnego. Na wybrane podejście mogą mieć wpływ różne uwarunkowania, takie jak krajowe i lokalne warunki i priorytety, lub potrzeba dostarczenia danych w celu wsparcia monitorowania wskaźników SPI.

5.2.2.2 Identyfikacja i zbieranie danych bezpieczeństwa powinny być dostosowane do potrzeb organizacji w zakresie skutecznego zarządzania bezpieczeństwem. W niektórych przypadkach proces zarządzania ryzykiem bezpieczeństwa uwypukli potrzebę dodatkowych danych bezpieczeństwa, aby lepiej ocenić wpływ (poziom prawdopodobieństwa i dotkliwość) oraz określić powiązane ryzyko. Podobnie, proces zarządzania poziomem bezpieczeństwa może uwydatnić potrzebę dodatkowych informacji w celu pełniejszego zrozumienia konkretnego problemu związanego z bezpieczeństwem lub ułatwienia ustanowienia lub udoskonalenia wskaźników SPI.

5.2.2.3 Podczas gromadzenia i wykorzystywania danych bezpieczeństwa i informacji bezpieczeństwa, należy wziąć pod uwagę ewentualne przypadki stronniczości. Na przykład język używany w dobrowolnych zgłoszeniach może czasami być emocjonalny lub mieć na celu osiągnięcie celów jednostki, co niekoniecznie musi leżeć w najlepszym interesie całej organizacji. W takich przypadkach informacje powinny być wykorzystywane w sposób rozsądny.

5.2.2.4 Państwa i podmioty lotnicze powinny rozważyć przyjęcie zintegrowanego podejścia do zbierania danych bezpieczeństwa pochodzących z różnych źródeł, zarówno wewnętrznych, jak i zewnętrznych. Integracja pozwala organizacjom uzyskać dokładniejszy obraz ryzyk bezpieczeństwa oraz osiągnąć w realizacji celów w zakresie bezpieczeństwa. Warto zauważyć, że dane bezpieczeństwa i informacje bezpieczeństwa, które początkowo wydają się nie mieć związku, mogą później okazać się kluczowe dla identyfikacji problemów związanych z bezpieczeństwem i wsparcia w podejmowaniu decyzji w oparciu o dane.

5.2.2.5 Wskazane jest usprawnienie ilości danych bezpieczeństwa i informacji bezpieczeństwa poprzez określenie, co szczególnie wspiera efektywne zarządzanie bezpieczeństwem w ich organizacji. Zebrane dane bezpieczeństwa i informacje bezpieczeństwa powinny wspierać wiarygodny pomiar wydajności systemu i ocenę znanych ryzyk, a także identyfikację pojawiających się ryzyk w ramach działalności organizacji. Wymagane dane bezpieczeństwa i informacje bezpieczeństwa będą zależały od wielkości i złożoności działań organizacji.

5.2.2.6 Rysunek 5-1 przedstawia przykłady typowych danych bezpieczeństwa i informacji bezpieczeństwa, które w wielu przypadkach są już dostępne. Koordynacja pomiędzy departamentami lub wydziałami jest niezbędna, aby usprawnić wysiłki w zakresie zgłaszania i zbierania danych bezpieczeństwa, aby uniknąć powielania.

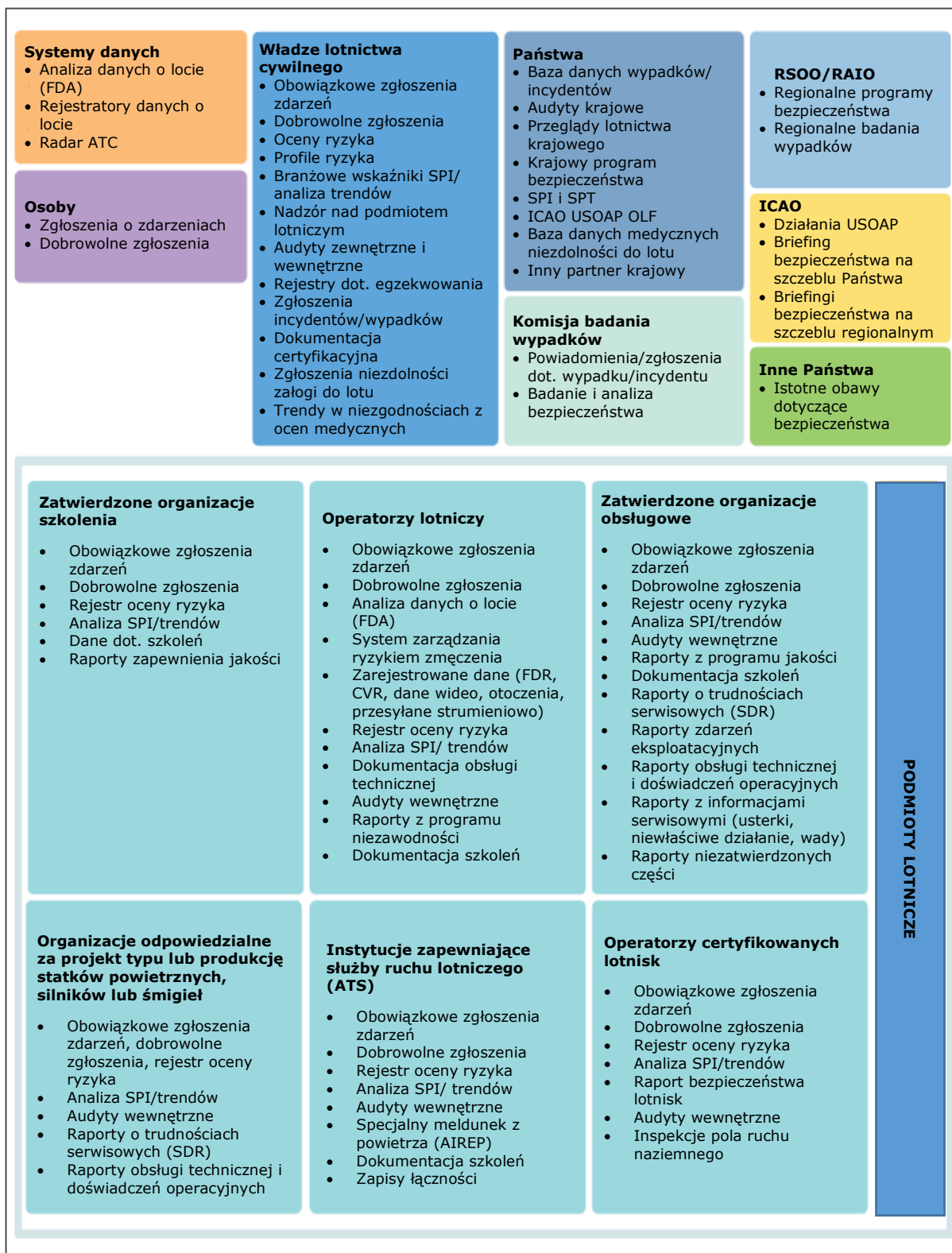
5.2.3 Badania wypadków i incydentów

Załącznik 13 wymaga od Państw ustanowienia i utrzymywania bazy danych o wypadkach i incydentach w celu ułatwienia skutecznej analizy informacji o faktycznych lub potencjalnych brakach w zakresie bezpieczeństwa oraz określenia wymaganych działań zapobiegawczych. Organy państwowe odpowiedzialne za wdrożenie SSP powinny mieć dostęp do państwowej bazy danych wypadków i incydentów w celu wsparcia w realizacji swoich obowiązków w zakresie bezpieczeństwa. Dodatkowe informacje, na których można oprzeć działania zapobiegawcze, mogą być zawarte w raportach końcowych dotyczących wypadków i incydentów, które zostały zbadane.

5.2.4 Badania w zakresie bezpieczeństwa prowadzone przez organy państwowe lub podmioty lotnicze

5.2.4.1 Zgodnie z przepisami Załącznika 13, Państwa są zobowiązane do badania wypadków, a także poważnych incydentów statków powietrznych o maksymalnej masie przekraczającej 2 250 kg, które miały miejsce na ich terytorium. Badania te są prowadzone przez państwowy organ ds. badania wypadków zgodnie z Załącznikiem 13. Prowadzenie takich badań może zostać przekazane innemu Państwu lub regionalnej organizacji badania wypadków i incydentów (RAIO) w drodze wzajemnego porozumienia i zgody.

5.2.4.2 Zachęca się do przeprowadzania badań w zakresie bezpieczeństwa poza tymi, które są wymagane zgodnie z Załącznikiem 13, ponieważ dostarczają one użytecznych informacji bezpieczeństwa w celu poprawy poziomu bezpieczeństwa. Dodatkowe informacje na temat badań realizowanych przez podmioty lotnicze znajdują się w Rozdziale 9.



Rysunek 5-1. Typowe źródła danych bezpieczeństwa i informacji bezpieczeństwa

5.2.5 Obowiązkowe systemy zgłaszania zdarzeń dotyczących bezpieczeństwa

5.2.5.1 Załącznik 19 wymaga od Państw ustanowienia obowiązkowego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa, który obejmuje, między innymi, zgłaszanie incydentów. Systemy zgłaszania opracowane przez Państwa i podmioty lotnicze powinny być tak proste, jak to tylko możliwe, w celu uzyskania dostępu, generowania i przesłania obowiązkowych zgłoszeń. Obowiązkowe systemy zgłaszania zdarzeń dotyczących bezpieczeństwa powinny mieć na celu zebranie wszystkich cennych informacji o zdarzeniu, w tym: co się stało, gdzie, kiedy i do kogo zgłoszenie jest kierowane. Ponadto obowiązkowe systemy zgłaszania zdarzeń dotyczących bezpieczeństwa powinny zapewniać zbieranie informacji o konkretnych zagrożeniach, o których wiadomo, że przyczyniają się do wypadków, co do których terminowa identyfikacja i informowanie są uważane za cenne (np. normalne warunki meteorologiczne, aktywność wulkaniczna itp.).

5.2.5.2 Niezależnie od zakresu obowiązkowego systemu zgłaszania zdarzeń, zaleca się, aby wszystkie obowiązkowo zebrane zgłoszenia były chronione zgodnie z zasadami opisanymi w Rozdziale 7.

5.2.5.3 Obowiązkowe systemy zgłaszania konkretnych zdarzeń mają tendencję do gromadzenia większej ilości informacji technicznych (np. dotyczących awarii sprzętu) aniżeli zgłaszania aspektów związanych z działaniami człowieka. Aby zaspokoić potrzebę szerszego zakresu zgłaszania zdarzeń dotyczących bezpieczeństwa, Państwa powinny również wdrożyć dobrowolny system zgłaszania zdarzeń dotyczących bezpieczeństwa. Ma on na celu zdobycie większej ilości informacji, takich jak aspekty związane z czynnikami ludzkimi, oraz zwiększenie bezpieczeństwa lotniczego.

Zgłaszanie wypadków i incydentów

5.2.5.4 Zgłaszanie wypadków i incydentów jest istotne dla wszystkich zainteresowanych stron działających w lotnictwie. Personel operacyjny jest zobowiązany do zgłaszania wypadków i niektórych rodzajów incydentów tak szybko, jak to możliwe, przy użyciu najszybszych środków dostępnych dla państwowego organu badającego wypadki lotnicze. Poważne incydenty muszą być zgłaszane, lista przykładów incydentów, które mogą być poważnymi incydentami znajduje się w Załączniku C do Załącznika 13.

5.2.5.5 Poniżej przedstawiono dwa główne aspekty, które należy wziąć pod uwagę przy podejmowaniu decyzji, czy dany incydent należy zaklasyfikować jako poważny incydent:

- a) Czy istniały okoliczności wskazujące na wysokie prawdopodobieństwo wypadku?
- b) Czy wypadku uniknięto tylko dzięki opatrności?

5.2.6 Dobrowolne systemy zgłaszania zdarzeń dotyczących bezpieczeństwa

5.2.6.1 Należy ustanowić dobrowolne systemy zgłaszania zdarzeń dotyczących bezpieczeństwa w celu zbierania danych bezpieczeństwa i informacji bezpieczeństwa, które nie zostały zebrane w ramach obowiązkowego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa. Zgłoszenia te wykraczają poza typowe zgłaszanie incydentów. Dobrowolne zgłoszenia mają tendencję do ujawniania stanów ukrytych, takich jak nieodpowiednie procedury lub przepisy bezpieczeństwa, błąd ludzki, itp. Jednym ze sposobów identyfikacji zagrożeń jest dobrowolne zgłaszanie.

5.2.6.2 Państwa powinny zapewniać ochronę danych bezpieczeństwa zebranych w ramach dobrowolnego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa i powiązanych źródeł oraz informacji bezpieczeństwa uzyskanych na podstawie tego systemu. Państwom i podmiotom lotniczym zaleca się zapoznanie się z Rozdziałem 7 w celu uzyskania wytycznych w jaki sposób zastosować ochronę do danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł. Odpowiednie zastosowanie ochrony zapewni ciągłą dostępność danych i informacji. Państwa powinny również rozważyć środki promujące dobrowolne zgłaszanie.

5.2.7 Przepisy dotyczące zgłaszania zdarzeń związanych z bezpieczeństwem specyficzne dla danego sektora

Przepisy dotyczące systemów zgłaszania zdarzeń związanych z bezpieczeństwem nieustannie ewoluują. Nowe wymagania dotyczące zgłaszania specyficzne dla poszczególnych sektorów, na przykład dotyczące zmęczenia i systemów bezałogowych statków powietrznych (RPAS), wprowadzono w ostatnim czasie w celu rozwiązania określonych problemów związanych z bezpieczeństwem oraz z pojawiającymi się nowymi rodzajami działalności lotniczej. Tabela 7 zawiera kilka przykładów systemów zgłaszania zdarzeń związanych z bezpieczeństwem specyficznych dla danego sektora znajdujących się w różnych Załącznikach, procedurach służb żeglugi powietrznej (PANS) i dokumentach.

Tabela 7. Przykłady systemów zgłaszania zdarzeń związanych z bezpieczeństwem specyficznych dla danego sektora znajdujących się w różnych Załącznikach, procedurach służb żeglugi powietrznej (PANS) i dokumentach

System zgłaszania	Odniesienie	Dla Państwa / podmiotu	Rok pierwszego przyjęcia / zatwierdzenia
Zgłaszanie badań wypadków i incydentów lotniczych	Załącznik 13 — <i>Badanie wypadków i incydentów lotniczych</i>	Państwo	1951
Zgłaszanie incydentów w ruchu lotniczym	PANS-ATM (Doc 4444), <i>Procedury służb żeglugi powietrznej – Zarządzanie ruchem lotniczym</i>	Państwo i podmiot lotniczy	1970
Zgłaszanie wypadków i incydentów z materiałami niebezpiecznymi	Załącznik 18 — <i>Bezpieczny transport materiałów niebezpiecznych drogą powietrzną</i>	Państwo	1981
Zgłaszanie trudności w obsłudze	Załącznik 8 — <i>Zdatność do lotu statków powietrznych</i>	Państwo	1982
Zgłaszanie incydentów w ruchu lotniczym	Doc 9426, <i>Podręcznik planowania służb ruchu lotniczego</i>	Podmiot lotniczy	1984
Zgłaszanie zderzeń z ptakami / zwierzęcą	Doc 9332, <i>Podręcznik systemu informacji o zderzeniach z ptakami ICAO (IBIS)</i>	Podmiot lotniczy	1989
	Załącznik 14 — <i>Lotniska, Tom I — Projektowanie i eksploatacja lotnisk</i>	Państwo i podmiot lotniczy	1990
	Doc 9137, <i>Podręcznik służb portu lotniczego, Część 3 – Kontrola i ograniczanie obecności zwierząt</i>	Państwo i podmiot lotniczy	1991
Zgłaszanie przypadków emisji laserowych	Doc 9815, <i>Podręcznik emiterów laserowych i bezpieczeństwa lotu</i>	Państwo	2003
Zgłaszanie przypadków zmęczenia	Załącznik 6 — <i>Eksploatacja statków powietrznych, Część I — Międzynarodowy zarobkowy transport lotniczy — Samoloty</i>	Podmiot lotniczy	2011
	Doc 9966, <i>Podręcznik nadzoru nad podejściami do zarządzania zmęczeniem</i>	Podmiot lotniczy	2012
Zgłaszanie trudności w obsłudze	Doc 9760, <i>Podręcznik zdatności do lotu</i>	Państwo	2014

Zgłaszanie zdarzeń związanych z bezpieczeństwem lotniska	Doc 9981, <i>Procedury służb żeglugi powietrznej (PANS) – Lotniska</i>	Podmiot lotniczy	2014
Systemy bezzałogowych statków powietrznych (RPAS)	Doc 10019, <i>Podręcznik systemów bezzałogowych statków powietrznych (RPAS)</i>	Podmiot lotniczy	2015
Przypadki niezdolności do pracy w locie i ustalenia ocen lekarskich	Załącznik 1 — Licencjonowanie personelu	Państwo	2016
Zgłaszanie wypadków i incydentów związanych z materiałami niebezpiecznymi	Doc 9284, <i>Instrukcje techniczne bezpiecznego transportu materiałów niebezpiecznych drogą powietrzną</i>	Państwo i podmiot lotniczy	2017

5.2.8 Ogólnodostępne systemy zgłaszania

Systemy zbierania danych bezpieczeństwa za pośrednictwem ogólnodostępnych systemów zgłaszania (ang. *self-disclosure systems*) obejmujących automatyczne zbieranie danych, w tym program działań w zakresie bezpieczeństwa lotniczego (ASAP) oraz programy analizy danych o locie (program zapewnienia jakości operacji lotniczych (FOQA), audyt bezpieczeństwa operacji liniowych (LOSA) oraz badanie bezpieczeństwa zwykłych operacji (NOSS)), są przykładami systemów, które zbierają dane bezpieczeństwa poprzez bezpośrednie obserwacje załóg lotniczych lub kontrolerów ruchu lotniczego, odpowiednio. Wszystkie te systemy pozwalają na rejestrację skutecznego działania systemu i człowieka. W celu uzyskania informacji na temat ochrony danych bezpieczeństwa i informacji bezpieczeństwa zebranych w ramach ogólnodostępnych systemów zgłaszania oraz ich źródeł, patrz Rozdział 7.

5.2.9 Wyniki inspekcji, audytów lub przeglądów

Wyniki interakcji pomiędzy przedstawicielami Państwa a podmiotami lotniczymi, takich jak inspekcje, audyty lub przeglądy, mogą również stanowić przydatny wkład w pulę danych bezpieczeństwa i informacji bezpieczeństwa. Dane bezpieczeństwa i informacje bezpieczeństwa uzyskane w trakcie tych interakcji można wykorzystać jako dowód skuteczności programu nadzoru.

5.2.10 Optymalne gromadzenie danych bezpieczeństwa i informacji bezpieczeństwa

Wiele danych bezpieczeństwa i informacji bezpieczeństwa wykorzystywanych jako podstawa podejmowania decyzji w oparciu o dane pochodzi z rutynowych, codziennych operacji realizowanych w ramach organizacji. Organizacja powinna najpierw określić, na jakie konkretne pytanie mają odpowiadać dane bezpieczeństwa i informacje bezpieczeństwa, lub jaki problem należy rozwiązać. Pomoże to określić odpowiednie źródło i wyjaśnić ilość potrzebnych danych lub informacji.

5.3. TAKSONOMIE

5.3.1 Najlepiej byłoby, gdyby dane bezpieczeństwa były kategoryzowane za pomocą taksonomii i definicji pomocniczych, aby dane mogły być zbierane i przechowywane przy użyciu znaczących terminów. Wspólne taksonomie i definicje ustanawiają standardowy język, poprawiając jakość informacji i komunikacji. Zdolność społeczności lotniczej do skupienia się na problemach związanych z bezpieczeństwem jest znacznie ulepszona dzięki wspólnemu językowi. Taksonomie umożliwiają analizę i ułatwiają wymianę informacji. Niektóre przykłady taksonomii obejmują:

- a) Model statku powietrznego: Organizacja może zbudować bazę danych ze wszystkimi certyfikowanymi modelami statków powietrznych.
- b) Lotnisko: Organizacja może używać kodów ICAO lub Międzynarodowego Stowarzyszenia Transportu Lotniczego (IATA) do identyfikacji lotnisk.
- c) Rodzaj zdarzenia: Organizacja może stosować taksonomie opracowane przez ICAO i inne międzynarodowe organizacje do klasyfikacji zdarzeń.

5.3.2 Istnieje wiele wspólnych taksonomii stosowanych w branży lotniczej. Oto kilka przykładów:

- a) ADREP: taksonomia kategorii zdarzeń, która stanowi część systemu ICAO dotyczącego zgłaszania wypadków i incydentów. Jest to kompilacja cech i powiązanych wartości, które pozwalają na analizę trendów w zakresie bezpieczeństwa w odniesieniu do tych kategorii.
- b) Zespół ds. bezpieczeństwa lotnictwa zarobkowego (CAST)/Zespół ds. taksonomii (CICTT) Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO): mający za zadanie opracowanie wspólnych taksonomii i definicji dla systemów zgłaszania wypadków i incydentów lotniczych.
- c) Grupa zadaniowa ds. wskaźników poziomu bezpieczeństwa (SPI-TF): mająca za zadanie opracowanie zharmonizowanej w skali globalnej metryki dla wskaźników SPI podmiotów lotniczych w ramach ich systemów SMS w celu zapewnienia jednolitych zasad w zbieraniu informacji i porównywaniu wyników analiz.

5.3.3 Wyciąg taksonomii opracowanej w ramach prac zespołu CICTT przedstawiono w Tabeli 8 wyłącznie jako przykład.

Tabela 8. Przykład typowej taksonomii

<i>Rodzaj działalności</i>	<i>Działania/ infrastruktura/system</i>	<i>Wartość</i>
Lotnisko, instytucja zapewniająca służby żeglugi powietrznej, operacje lotnicze, organizacja obsługowa, organizacja projektująca i produkująca	Władza lotnicza	Brak, złe lub nieskuteczne ustawodawstwo i/lub regulacje
		Nieskuteczne możliwości badania wypadków lub ich brak
		Niewystarczające możliwości sprawowania nadzoru
	Kierownictwo	Ograniczone zaangażowanie kierownictwa lub jego brak – Kierownictwo nie wykazuje poparcia dla działań
		Brak lub niepełny opis ról, odpowiedzialności i obowiązków
		Ograniczona dostępność zasobów lub ograniczone planowanie, w tym obsada personalna lub ich brak
		Nieskuteczne polityki lub ich brak
		Niepoprawne lub niekompletne procedury, w tym instrukcje
		Złe zarządzanie i relacje pracy lub ich brak
		Nieskuteczna struktura organizacyjna lub jej brak
		Słaba kultura bezpieczeństwa organizacji
		Nieskuteczne procedury audytowe lub ich brak
		Ograniczona alokacja zasobów lub jej brak

5.3.4 Szczególnie ważne są taksonomie zagrożeń. Identyfikacja zagrożenia jest często pierwszym krokiem w procesie zarządzania ryzykiem. Rozpoczęcie od powszechnie uznanego języka sprawia, że dane bezpieczeństwa

są bardziej znaczące, łatwiejsze do sklasyfikowania i prostsze do przetworzenia. Struktura taksonomii zagrożeń może obejmować komponent ogólny i szczegółowy.

5.3.5 Komponent ogólny pozwala użytkownikom uchwycić charakter zagrożenia co ma pomóc w identyfikacji, analizie i kodowaniu. Zespół CICTT opracował taksonomię zagrożeń, która klasyfikuje zagrożenia według dziedzin zagrożeń (środowiskowe, techniczne, organizacyjne i ludzkie).

5.3.6 Komponent szczegółowy precyzuje definicję i kontekst zagrożenia. Umożliwia on bardziej szczegółowe przetwarzanie zarządzania ryzykiem. Poniższe kryteria mogą być pomocne przy formułowaniu definicji zagrożeń. Nadając nazwę zagrożeniu, należy uwzględnić aby była ono:

- a) wyraźnie rozpoznawalne;
- b) opisane w pożądanym (kontrolowanym) stanie; oraz
- c) zidentyfikowane przy użyciu przyjętych nazw.

5.3.7 Wspólne taksonomie mogą nie zawsze być dostępne dla poszczególnych baz danych. W takim przypadku należy zastosować mapowanie danych w celu umożliwienia standaryzacji danych bezpieczeństwa i informacji bezpieczeństwa w oparciu o równoważność. Stosując przykład typu statku powietrznego, mapowanie danych może wykazać, że „Boeing 787-8” w jednej bazie danych jest równoważny z „788” w innej. Może to nie być prosty proces, ponieważ poziom szczegółowości danych i informacji bezpieczeństwa na etapie zbierania danych może się różnić. Większość systemów SDCPS będzie skonfigurowanych w taki sposób, aby wspomagać standaryzację w zbieraniu danych, zmniejszając obciążenie przy mapowaniu danych.

5.4. PRZETWARZANIE DANYCH BEZPIECZEŃSTWA

Przetwarzanie danych bezpieczeństwa odnosi się do manipulowania danymi bezpieczeństwa w celu uzyskania znaczących informacji bezpieczeństwa w przydatnych formach, takich jak diagramy, raporty lub tabele. Istnieje szereg ważnych kwestii związanych z przetwarzaniem danych bezpieczeństwa, w tym: jakość, agregacja, fuzja i filtrowanie danych.

5.4.1 Jakość danych

5.4.1.1 Jakość danych odnosi się do danych, które są czyste i nadają się do określonego celu. Jakość danych obejmuje następujące aspekty:

- a) czystość;
- b) znaczenie;
- c) terminowość; oraz
- d) dokładność i poprawność.

5.4.1.2 Czyszczenie danych to proces wykrywania i korygowania (lub usuwania) zniekształconych lub niedokładnych zapisów z zestawu rekordów, tabeli lub bazy danych polegający na identyfikowaniu niekompletnych, niepoprawnych, niedokładnych lub nieistotnych części danych, a następnie zastępowaniu, modyfikowaniu lub usuwaniu zanieczyszczonych lub nieobrobionych danych.

5.4.1.3 Istotne dane to dane, które spełniają potrzeby organizacji i dotyczą ich najważniejszych problemów. Organizacja powinna ocenić znaczenie danych w oparciu o swoje potrzeby i działania.

5.4.1.4 Terminowość danych bezpieczeństwa i informacji bezpieczeństwa stanowi funkcję ich aktualności. Dane wykorzystywane do podejmowania decyzji powinny odzwierciedlać zdarzenia mające miejsce możliwie jak najbliżej czasu rzeczywistego. Częstym przypadkiem jest konieczność oceny w oparciu o zmieniającą się sytuację. Na przykład, dane zebrane dwa lata temu na typie statku powietrznego nadal działającego na tej samej trasie, bez wprowadzania znaczących zmian, mogą zapewnić terminowe odzwierciedlenie sytuacji. Podczas gdy dane zebrane tydzień temu na typie statku powietrznego, który nie jest już w użyciu, nie mogą dostarczyć znaczącego, aktualnego odzwierciedlenia obecnej rzeczywistości.

5.4.1.5 Dokładność danych odnosi się do wartości, które są poprawne i odzwierciedlają opisany scenariusz. Niedokładność danych często występuje kiedy użytkownicy wprowadzają błędną wartość lub popełniają błąd typograficzny. Problem ten można przezwyciężyć poprzez posiadanie wykwalifikowanego i przeszkolonego personelu do wprowadzania danych lub poprzez posiadanie elementów w aplikacji, takich jak sprawdzanie pisowni. Wartości danych mogą z upływem czasu stać się niedokładne, co znane jest jako „rozkład danych”. Ruch jest kolejną przyczyną niedokładnych danych. Ponieważ dane są wyodrębniane, przekształcane i przenoszone z jednej bazy danych do drugiej, mogą być w pewnym stopniu zmienione, zwłaszcza jeżeli oprogramowanie nie jest niezawodne.

5.4.2 Agregacja danych bezpieczeństwa i informacji bezpieczeństwa

Agregacja danych ma miejsce, kiedy dane bezpieczeństwa i informacje bezpieczeństwa są zbierane i przechowywane w systemie SDCPS organizacji i wyrażane w formie skróconej do celu analizy. Agregacja danych bezpieczeństwa i informacji bezpieczeństwa polega na zgromadzeniu ich razem, w wyniku czego powstanie większy zbiór danych. W przypadku systemu SDCPS poszczególne elementy danych bezpieczeństwa są agregowane w bazie danych bez dawania pierwszeństwa jednym danym przed innymi. Powszechnym celem agregacji jest uzyskanie informacji o określonej grupie lub rodzaju działalności w oparciu o określone zmienne takie jak lokalizacja, typ floty lub grupa zawodowa. Agregacja danych może być czasami pomocna w wielu organizacjach lub regionach, które nie mają wystarczającej ilości danych, aby zapewnić odpowiednią anonimizację w celu ochrony źródeł danych dotyczących bezpieczeństwa i informacji dotyczących bezpieczeństwa oraz w celu wsparcia analizy.

5.4.3 Fuzja danych

Fuzja danych to proces łączenia wielu zbiorów danych dotyczących bezpieczeństwa w celu uzyskania bardziej spójnych, połączonych i użytecznych danych bezpieczeństwa aniżeli dane zapewniane przez dowolny zbiór danych bezpieczeństwa. Integracja zbiorów danych bezpieczeństwa, a następnie ich zmniejszenie lub zastąpienie, zwiększa niezawodność i użyteczność danych. Na przykład, dane z systemów FDA operatorów lotniczych mogłyby zostać połączone z danymi meteorologicznymi i danymi radarowymi w celu uzyskania bardziej użytecznego zbioru danych do dalszego przetwarzania.

5.4.4 Filtrowanie danych bezpieczeństwa i informacji bezpieczeństwa

Filtrowanie danych dotyczących bezpieczeństwa odnosi się do szerokiej gamy strategii lub rozwiązań mających za zadanie doskonalenie zbiorów danych bezpieczeństwa. Oznacza to, że zbiory danych są dopracowywane do formy jakiej potrzebuje decydent, bez uwzględniania innych danych, które mogą być powtarzalne, nieistotne lub nawet wrażliwe. Różne typy filtrów danych mogą być używane do generowania raportów lub prezentowania danych w sposób ułatwiający porozumiewanie się.

5.5. ZARZĄDZANIE DANYMI BEZPIECZEŃSTWA I INFORMACJAMI BEZPIECZEŃSTWA

5.5.1 Zarządzanie danymi bezpieczeństwa i informacjami bezpieczeństwa można zdefiniować jako opracowanie, wykonanie i nadzór nad planami, politykami, programami i praktykami, które zapewniają ogólną integralność, dostępność, użyteczność i ochronę danych bezpieczeństwa i informacji bezpieczeństwa wykorzystywanych przez organizację.

5.5.2 Zarządzanie danymi bezpieczeństwa i informacjami dotyczącymi bezpieczeństwa, które obejmuje niezbędne funkcje, zapewni, że dane bezpieczeństwa i informacje bezpieczeństwa organizacji będą zbierane, przechowywane, analizowane, zachowywane i archiwizowane, a także zarządzane, chronione i udostępniane zgodnie z przeznaczeniem. W ramach zarządzania, należy w szczególności zidentyfikować:

- a) jakie dane będą zbierane;
- b) definicje danych, taksonomię i formaty;
- c) sposób zbierania, zestawiania i integracji danych z innymi źródłami danych bezpieczeństwa i informacji bezpieczeństwa;
- d) sposób, w jaki dane bezpieczeństwa i informacje bezpieczeństwa będą przechowywane, archiwizowane i zabezpieczane; na przykład, struktura bazy danych, a w przypadku systemu IT, architektura wspierająca;
- e) sposób wykorzystania danych bezpieczeństwa i informacji bezpieczeństwa;
- f) sposób udostępniania i wymiany informacji z innymi stronami;
- g) sposób ochrony danych bezpieczeństwa i informacji bezpieczeństwa, odpowiednio do specyfiki typu i źródła danych bezpieczeństwa i informacji bezpieczeństwa; oraz
- h) sposób pomiaru i utrzymywania jakości.

5.5.3 Bez jasno zdefiniowanych procesów dotyczących tworzenia informacji bezpieczeństwa, organizacja nie może osiągnąć wiarygodnych i spójnych informacji, na podstawie których podejmowane są decyzje w oparciu o dane.

5.5.4 Panowanie nad danymi

Panowanie nad danymi to uprawnienia, kontrola i podejmowanie decyzji dotyczących procesów i procedur wspierających działania organizacji w zakresie zarządzania danymi. Określa, w jaki sposób dane bezpieczeństwa i informacje bezpieczeństwa są zbierane, analizowane, używane, udostępniane i chronione. Panowanie nad danymi zapewnia, że system zarządzania danymi daje pożądaną efekt dzięki kluczowym cechom integralności, dostępności, użyteczności i ochrony, jak opisano poniżej.

Integralność – Integralność danych odnosi się do wiarygodności źródeł, informacji i zdarzeń. Jednak integralność danych obejmuje utrzymanie i zapewnienie dokładności i spójności danych w całym cyklu życia. Jest to krytyczny aspekt projektowania, wdrażania i użytkowania systemu SDCPS podczas przechowywania, przetwarzania lub pobierania danych.

Dostępność – Należy sprecyzować kto ma pozwolenie na używanie lub udostępnianie przechowywanych danych bezpieczeństwa i informacji bezpieczeństwa. Musi to uwzględniać porozumienie pomiędzy właścicielem danych/informacji a wyznaczonym podmiotem odpowiedzialnym za ochronę. W przypadku podmiotów, które mogą korzystać z danych, należy sprecyzować sposób dostępu i przetwarzania danych.

Istnieje wiele technik maksymalizacji dostępności danych, w tym redundancja miejsc przechowywania oraz metody i narzędzia dostępu do danych.

Użyteczność – Aby zmaksymalizować zwrot z danych bezpieczeństwa i informacji bezpieczeństwa, ważne jest również uwzględnienie standardów użyteczności. Ludzie nieustannie wchodzą w interakcję z danymi bezpieczeństwa i informacjami bezpieczeństwa w miarę ich pozyskiwania. Organizacje powinny ograniczać do minimum błędy ludzkie, ponieważ stosowane są aplikacje automatyzacji. Narzędzia zwiększające użyteczność obejmują słowniki danych i bazy metadanych. Wraz z rozwojem interakcji człowieka w kierunku zastosowania dużych zbiorów danych i procesów uczenia maszynowego, coraz ważniejsze będzie lepsze zrozumienie ludzkiej użyteczności, ponieważ ma ona zastosowanie do maszyn w celu zminimalizowania błędów w obliczeniach w danych bezpieczeństwa i informacjach bezpieczeństwa w przyszłości.

Ochrona – Państwa powinny zapewnić, że dane bezpieczeństwa, informacje bezpieczeństwa i powiązane źródła są odpowiednio chronione. Więcej informacji znajduje się w Rozdziale 7.

5.5.5 Zarządzanie metadanymi

5.5.5.1 Metadane definiuje się jako zbiór danych opisujących i przekazujących informacje o innych danych, innymi słowy, są to dane na temat danych. Korzystanie ze standardów metadanych zapewnia wspólne znaczenie lub definicję danych. Zapewnia właściwe użytkowanie i interpretację przez właścicieli i użytkowników, a dane są łatwo pobierane do analizy.

5.5.5.2 Ważne jest, aby organizacje katalogowały swoje dane na podstawie ich właściwości, w tym między innymi:

- a) czego dane dotyczą;
- b) skąd pochodzą (oryginalne źródło);
- c) kto je stworzył;
- d) kiedy zostały utworzone;
- e) kto je używał;
- f) do czego służą;
- g) częstotliwość zbierania; oraz
- h) wszelkie przypadki przetwarzania lub transformacji.

5.5.5.3 Metadane zapewniają powszechne zrozumienie tego, czym są dane, oraz zapewniają prawidłowe użytkowanie i interpretację przez właścicieli i użytkowników. Mogą one również identyfikować błędy w gromadzeniu danych, co prowadzi do ciągłych ulepszeń programu.

ROZDZIAŁ 6

ANALIZA BEZPIECZEŃSTWA

6.1. WSTĘP

6.1.1 Analiza bezpieczeństwa to proces stosowania technik statystycznych lub innych technik analitycznych w celu sprawdzenia, zbadania, opisanego, przekształcenia, skondensowania, oceny i wizualizacji danych bezpieczeństwa i informacji bezpieczeństwa w celu uzyskania przydatnych informacji, zasugerowania wniosków oraz zapewnienia wsparcia w podejmowaniu decyzji w oparciu o dane. Analiza pomaga organizacjom generować przydatne informacje bezpieczeństwa w postaci statystyk, wykresów, map, tablic i prezentacji. Analiza bezpieczeństwa jest szczególnie cenna dla dużych i/lub dojrzałych organizacji o bogatych danych bezpieczeństwa. Analiza bezpieczeństwa opiera się na jednoczesnym stosowaniu statystyk, obliczeń i badań operacyjnych. Wynik analizy bezpieczeństwa powinien przedstawiać sytuację w zakresie bezpieczeństwa w sposób umożliwiający decydentom podejmowanie decyzji dotyczących bezpieczeństwa w oparciu o dane.

6.1.2 Państwa są zobowiązane do ustanowienia i utrzymywania procesu analizy danych bezpieczeństwa i informacji bezpieczeństwa pochodzących z systemu SDCPS i powiązanych baz danych bezpieczeństwa. Jednym z celów analizy danych bezpieczeństwa i informacji bezpieczeństwa na poziomie Państwa jest identyfikacja zagrożeń systemowych i przekrojowych, które w innym razie nie zostaną zidentyfikowane w ramach procesów analizy danych bezpieczeństwa poszczególnych podmiotów lotniczych.

6.1.3 Analiza bezpieczeństwa może być nową funkcją, którą Państwo lub podmiot lotniczy będą musieli ustanowić. Należy zauważyć, że wymagane kompetencje do prowadzenia skutecznej analizy bezpieczeństwa mogą być poza zakresem tradycyjnego inspektora bezpieczeństwa. Państwa i podmioty powinny rozważyć umiejętności niezbędne do analizy informacji bezpieczeństwa i zdecydować, czy rola ta, przy odpowiednim przeszkoleniu, powinna być poszerzeniem obecnego stanowiska, czy też bardziej skuteczne byłoby ustanowienie nowego stanowiska, outsourcingu roli lub zastosowanie połączenia tych podejść. Decyzja będzie zależała od planów i sytuacji każdego Państwa lub podmiotu lotniczego.

6.1.4 Równoległe z rozważaniami na temat zasobów ludzkich należy przeprowadzić analizę istniejącego oprogramowania oraz polityki i procesów biznesowych i decyzyjnych. Aby była skuteczna, analiza bezpieczeństwa powinna być zintegrowana z istniejącymi podstawowymi narzędziami, politykami i procesami organizacji. Po połączeniu, ciągły rozwój inteligencji bezpieczeństwa powinien być płynny i powinien stanowić część zwykłej praktyki biznesowej organizacji.

6.1.5 Analiza danych bezpieczeństwa i informacji bezpieczeństwa może być przeprowadzona na wiele sposobów, niektóre wymagają bardziej niezawodnych danych i zdolności analitycznych niż inne. Wykorzystanie odpowiednich narzędzi do analizy danych bezpieczeństwa i informacji bezpieczeństwa zapewnia dokładniejsze zrozumienie ogólnej sytuacji poprzez badanie danych w sposób, który ujawnia istniejące relacje, powiązania, wzorce i trendy, które istnieją wewnątrz.

6.1.6 Organizacja o dojrzałej zdolności analitycznej jest w stanie lepiej:

- a) ustanowić skuteczny pomiar wskaźników bezpieczeństwa;
- b) ustanowić możliwości prezentacji bezpieczeństwa (np. tablicy bezpieczeństwa) w celu łatwej interpretacji informacji bezpieczeństwa przekazywanych przez decydentów;
- c) monitorować poziom bezpieczeństwa danego sektora, organizacji, systemu lub procesu;

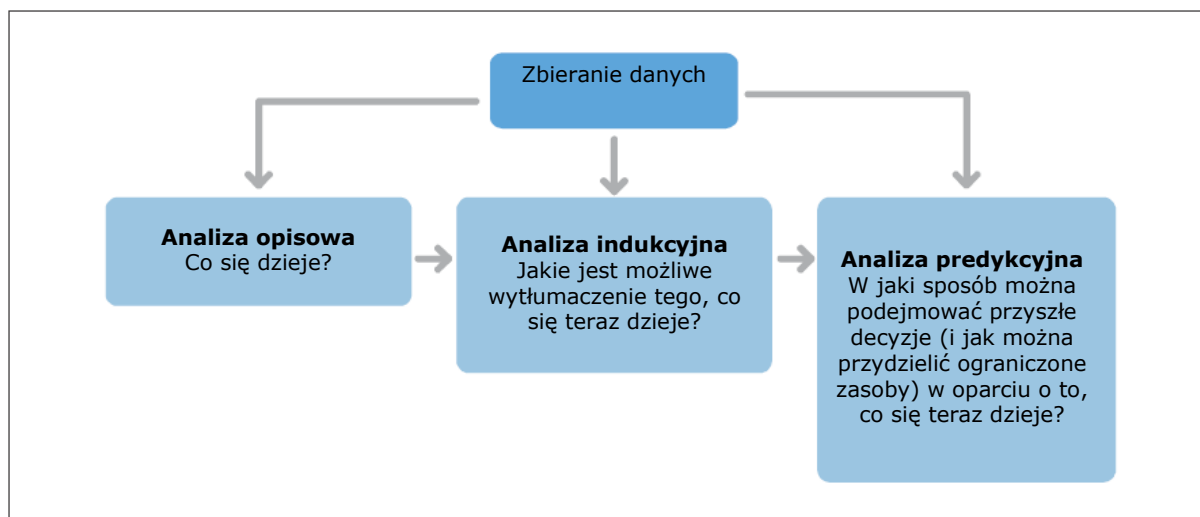
- d) podkreślić trendy w zakresie bezpieczeństwa, szczegółowe cele bezpieczeństwa;
- e) ostrzegać decydentów ds. bezpieczeństwa w oparciu o czynniki uruchamiające bezpieczeństwo;
- f) identyfikować czynniki, które powodują zmianę;
- g) identyfikować połączenia lub „korelacje” pomiędzy różnymi czynnikami;
- h) testować założenia; oraz
- i) rozwijać możliwości modelowania predykcyjnego.

6.1.7 Wykonując analizę bezpieczeństwa organizacje powinny uwzględnić szereg odpowiednich źródeł informacji, a nie tylko „dane bezpieczeństwa”. Przykłady przydatnych dodatków do zbioru danych to: pogoda, teren, ruch, demografia, geografia, itp. Dostęp do szerszego zakresu źródeł danych i korzystanie z nich zapewni analitykom i decydentom ds. bezpieczeństwa świadomość w obrębie większego zakresu, w ramach którego podejmowane są decyzje dotyczące bezpieczeństwa.

6.1.8 Państwa powinny być szczególnie zainteresowane informacjami, które identyfikują trendy i zagrożenia w zakresie bezpieczeństwa, które występują w całym systemie lotniczym.

6.2. RODZAJE ANALIZY

Analiza danych bezpieczeństwa i informacji bezpieczeństwa pozwala również decydentom na porównanie informacji z innymi grupami (tj. grupą kontrolną lub porównawczą), aby pomóc wyciągnąć wnioski z danych bezpieczeństwa. Typowe podejścia obejmują analizę opisową (opisywanie), analizę indukcyjną (wnioskowanie) i analizę predykcyjną (przewidywanie), jak przedstawiono na Rysunku 6-1.



Rysunek 6-1. Powszechne rodzaje analizy statystycznej

6.2.1 Analiza opisowa

6.2.1.1 Statystyka opisowa służy do opisu lub podsumowania danych w sposób znaczący i użyteczny. Pomaga ona w opisywaniu, przedstawianiu lub podsumowywaniu danych w taki sposób, aby z danych mogły wyłonić się szablony, które zapewnią pomoc w jasnym definiowaniu studiów przypadku, możliwości i wyzwań. Techniki opisowe dostarczają informacji o danych, jednak nie pozwalają użytkownikom na wyciąganie wniosków

poza analizowanymi danymi lub na wyciąganie wniosków dotyczących hipotez na temat danych. Stanowią one sposób na opisanie danych.

6.2.1.2 Statystyka opisowa jest pomocna, ponieważ jeżeli przedstawiamy tylko surowe dane, szczególnie w dużych ilościach, trudno byłoby sobie wyobrazić, co dane nam przedstawiają. Statystyka opisowa umożliwia użytkownikom prezentowanie i przeglądanie danych w bardziej znaczący sposób, umożliwiając prostszą interpretację danych. Narzędzia takie jak tabele i macierze, wykresy, a nawet mapy są przykładem narzędzi używanych do podsumowania danych. Statystyka opisowa obejmuje pomiar tendencji centralnej takiej jak średnia (przeciętna), mediana i tryb, a także pomiar zmienności takiej jak zakres, kwartyle, minimum i maksimum, rozkłady częstotliwości, wariancja i odchylenie standardowe (SD). Podsumowania te mogą być albo początkową podstawą do opisywania danych w ramach bardziej szczegółowej analizy statystycznej, albo same w sobie wystarczą do konkretnego badania.

6.2.2 Analiza indukcyjna

Statystyka indukcyjna ma na celu wykorzystanie danych do poznania większej populacji, którą reprezentuje próbka danych. Zbadanie każdego elementu całej populacji oraz dostęp do całej populacji nie zawsze jest wygodny i możliwy. Statystyka indukcyjna to techniki, które pozwalają użytkownikom danych na formułowanie uogólnień i wniosków na temat populacji, z której pobrano próbki w celu opisanie trendów. Obejmują one metody oszacowania parametrów, testowania hipotez statystycznych, porównywania średniej wydajności dwóch grup w tym samym pomiarze w celu zidentyfikowania różnic lub podobieństw, oraz metody identyfikacji możliwych korelacji i zależności pomiędzy zmiennymi.

6.2.3 Analiza predykcyjna

Inne rodzaje analiz obejmują analizy prawdopodobieństwa lub analizy predykcyjne, które wyodrębniają informacje z danych historycznych i danych bieżących oraz wykorzystują je do przewidywania trendów i wzorców zachowań. Wzorce znalezione w danych pomagają zidentyfikować pojawiające się ryzyka i możliwości. Często nieznanym wydarzeniem będącym przedmiotem zainteresowania jest wydarzenie w przyszłości, ale analiza predykcyjna może być stosowana do dowolnego typu nieznanego wydarzenia w przeszłości, teraźniejszości lub przyszłości. Rdzeń analizy predykcyjnej polega na wychwytywaniu relacji pomiędzy zmiennymi z poprzednich zdarzeń i wykorzystywaniu ich do przewidywania nieznanego wyniku. Niektóre systemy umożliwiają użytkownikom modelowanie różnych scenariuszy ryzyka lub możliwości o różnych wynikach. Umożliwia to decydentom ocenę decyzji, które mogą podejmować w obliczu różnych nieznanych okoliczności, oraz ocenę sposobu, w jaki mogą skutecznie przydzielić ograniczone zasoby do obszarów, w których istnieje najwyższe ryzyko lub najlepsze możliwości.

6.2.4 Analiza połączona

6.2.4.1 Różne rodzaje analiz statystycznych są ze sobą powiązane i często prowadzone razem. Na przykład technika indukcyjna może być głównym narzędziem wykorzystywanym do wyciągania wniosków dotyczących zbioru danych, ale statystyka opisowa jest także używana i prezentowana. Również wyniki statystyki indukcyjnej są często wykorzystywane jako podstawa analizy predykcyjnej.

6.2.4.2 Techniki analityczne można zastosować do analizy bezpieczeństwa w celu:

- a) identyfikacji przyczyn i czynników przyczyniających się do zagrożeń oraz elementów, które są szkodliwe dla ciągłej poprawy bezpieczeństwa;
- b) zbadania obszarów wymagających poprawy i zwiększenia skuteczności środków kontroli bezpieczeństwa; oraz
- c) wsparcia bieżącego monitorowania poziomu bezpieczeństwa i trendów.

6.3. RAPORTOWANIE WYNIKÓW ANALIZY

6.3.1 Wyniki analizy danych bezpieczeństwa mogą uwydatnić obszary wysokiego ryzyka oraz pomóc decydom i menedżerom w:

- a) podejmowaniu natychmiastowych działań naprawczych;
- b) wdrożeniu nadzoru w oparciu o ryzyko bezpieczeństwa;
- c) zdefiniowaniu lub udoskonaleniu polityki bezpieczeństwa lub celów w zakresie bezpieczeństwa;
- d) zdefiniowaniu lub udoskonaleniu wskaźników SPI;
- e) zdefiniowaniu lub udoskonaleniu poziomów SPT;
- f) określeniu czynników uruchamiających wskaźniki SPI;
- g) promowaniu bezpieczeństwa; oraz
- h) prowadzeniu dalszej oceny ryzyka bezpieczeństwa.

6.3.2 Wyniki analizy bezpieczeństwa powinny zostać udostępnione zainteresowanym stronom z dziedziny bezpieczeństwa lotniczego w sposób, który można łatwo zrozumieć. Wyniki powinny być prezentowane odbiorcom, takim jak decydenci w organizacji, zewnętrzne podmioty lotnicze, władze lotnicze i inne Państwa. Wyniki analizy bezpieczeństwa można przedstawić na kilka sposobów, oto kilka przykładów:

- a) Bezpośrednie zagrożenie bezpieczeństwa: do przekazania innym Państwom lub podmiotom lotniczym zagrożeń bezpieczeństwa o potencjalnych skutkach, które mogą być katastrofalne i które wymagają natychmiastowych działań.
- b) Raporty z analiz bezpieczeństwa: zazwyczaj przedstawiają informacje ilościowe i jakościowe wraz z jasnym opisem zakresu i źródła niepewności w związku z wnioskami analizy. Raporty te mogą również zawierać odpowiednie zalecenia bezpieczeństwa.
- c) Konferencje bezpieczeństwa: dla państw i podmiotów lotniczych w celu udostępniania informacji bezpieczeństwa i wyników analiz bezpieczeństwa, które mogą promować inicjatywy współpracy.

6.3.3 Pomocne jest przełożenie zaleceń na plany działania, decyzje i priorytety, które decydenci w organizacji muszą wziąć pod uwagę oraz, jeżeli to możliwe, nakreślić, kto i co powinien zrobić z wynikami analizy i do kiedy.

6.3.4 Narzędzia wizualizacji, takie jak wykresy, zobrazowania i tablice, są prostymi, ale skutecznymi sposobami prezentacji wyników analizy danych. Kilka przykładów raportów z wizualnych analiz danych można znaleźć w zintegrowanym systemie analizy i zgłaszania trendów dotyczących bezpieczeństwa ICAO (iSTARS) na stronie <https://icao.int/safety/iSTARS>.

6.3.5 Tablice bezpieczeństwa

6.3.5.1 Poziom bezpieczeństwa organizacji powinien być widoczny i powinien jasno wskazywać wszystkim zainteresowanym stronom, że bezpieczeństwo jest skutecznie zarządzane. Jednym z podejść do pokazania tego jest „tablica bezpieczeństwa”, która jest wizualną reprezentacją zapewniającą kadrze kierowniczej, menedżerom i specjalistom ds. bezpieczeństwa szybki i łatwy sposób na sprawdzenie poziomu bezpieczeństwa organizacji.

6.3.5.2 Oprócz zobrazowania SPI i SPT organizacji w czasie rzeczywistym, tablice bezpieczeństwa mogą również zawierać informacje dotyczące kategorii, przyczyny i dotkliwości konkretnych zagrożeń. Najlepiej byłoby, gdyby informacje prezentowane na tablicy można było dostosować w taki sposób, aby prezentować informacje

wymagane do zapewnienia wsparcia w podejmowaniu decyzji na różnych szczeblach organizacji. Użycie czynników uruchamiających jest przydatne do dostarczania podstawowych informacji wizualnych, aby podkreślić, czy są jakieś kwestie, które należy rozwiązać w przypadku konkretnego wskaźnika. Analitycy i decydenci będą chcieli dysponować możliwością konfigurowania tablicy w taki sposób, aby przedstawiała najważniejsze wskaźniki, a także funkcją, która pozwoli im na dokładne zapoznanie się ze sposobem pomiaru.

6.3.5.3 Zbieranie i analizowanie danych wymagane do skutecznego zarządzania i podejmowania decyzji jest procesem ciągłym. Wyniki analizy danych mogą ujawnić, że konieczne jest zbieranie i analizowanie danych w większej ilości i o lepszej jakości w celu wsparcia działań i decyzji, które organizacja musi podjąć. Rysunek 6-2 pokazuje, w jaki sposób raportowanie wyników analizy może określać dalsze wymagania dotyczące zbierania danych.

6.4. UDOSTĘPNIANIE I WYMIANA INFORMACJI BEZPIECZEŃSTWA

Bezpieczeństwo można poprawić, kiedy informacje bezpieczeństwa są udostępniane lub wymieniane. Zapewnia to spójną, opartą na danych i przejrzystą odpowiedź na obawy dotyczące bezpieczeństwa na poziomie globalnym, krajowym i organizacyjnym. Udostępnianie informacji bezpieczeństwa odnosi się do dawania, podczas gdy wymiana odnosi się do dawania i otrzymywania w zamian.

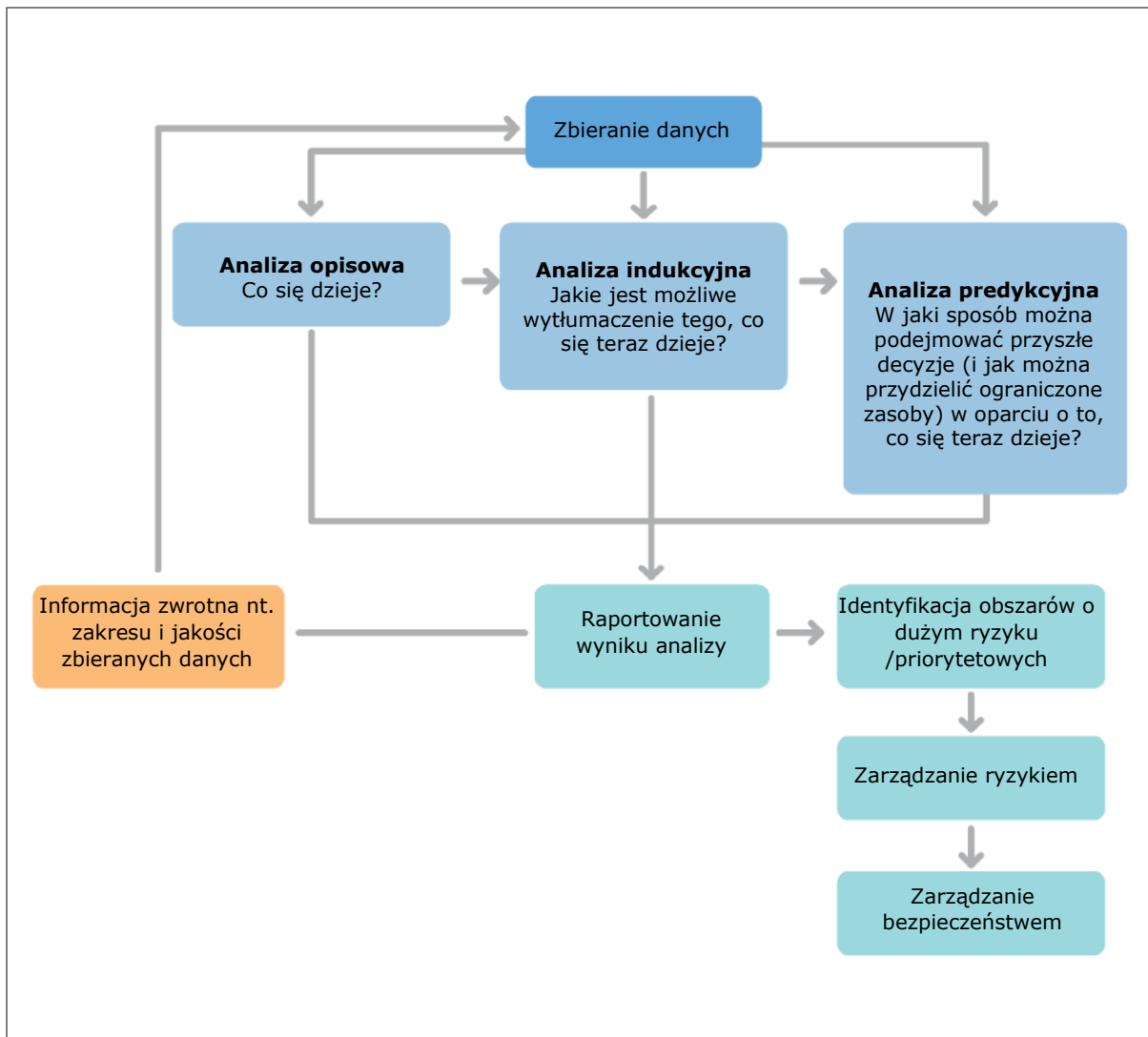
6.4.1 Udostępnianie w obrębie Państwa

6.4.1.1 Państwa powinny promować tworzenie sieci udostępniania lub wymiany informacji bezpieczeństwa pomiędzy użytkownikami systemu lotniczego, oraz ułatwiać udostępnianie i wymianę informacji bezpieczeństwa, chyba że ich prawo krajowe stanowi inaczej. Wytyczne dotyczące promocji bezpieczeństwa dla Państw i podmiotów lotniczych przedstawiono w Rozdziale 8 i 9, odpowiednio.

6.4.1.2 Poziom ochrony i warunki, na jakich informacje bezpieczeństwa będą udostępniane lub wymieniane pomiędzy organami krajowymi i podmiotami lotniczymi, muszą być zgodne z prawem krajowym. Dalsze informacje na temat ochrony danych bezpieczeństwa i informacji bezpieczeństwa znajdują się w Rozdziale 7.

6.4.2 Udostępnianie pomiędzy Państwami

Państwa powinny jak najszybciej udostępniać informacje bezpieczeństwa innym Państwom, jeżeli w analizie informacji zawartych w systemie SDCPS zidentyfikowane zostaną problemy związane z bezpieczeństwem, które mogą być w obszarze zainteresowania innego Państwa. Państwa zachęca się również do udostępniania informacji bezpieczeństwa w ramach grupy RASG. Przed udostępnieniem informacji bezpieczeństwa Państwa powinny zapewnić, że poziom ochrony i warunki, na jakich informacje bezpieczeństwa będą udostępniane, są zgodne z Załącznikiem 19, Dodatek 3. Szczegółowe wytyczne znajdują się w Rozdziale 7.



Rysunek 6-2. Integracja procesu D3M z zarządzaniem bezpieczeństwem

6.5. PODEJMOWANIE DECYZJI W OPARCIU O DANE

6.5.1 Podstawowym celem analizy bezpieczeństwa i zgłaszania zdarzeń dotyczących bezpieczeństwa jest przedstawienie decydentom obrazu sytuacji w zakresie bezpieczeństwa, który umożliwi im podejmowanie decyzji na podstawie przedstawionych danych. Jest to znane jako podejmowanie decyzji w oparciu o dane (określane również jako DDDM [ang. *data-driven decision-making*] lub D3M), podejście procesowe do podejmowania decyzji.

6.5.2 Wiele zdarzeń lotniczych wynikało, przynajmniej częściowo, ze złych decyzji kierownictwa, które mogą prowadzić do marnotrawstwa pieniędzy, pracy i zasobów. Celem decydentów ds. bezpieczeństwa jest, w perspektywie krótkoterminowej, ograniczenie do minimum słabych wyników i osiągnięcie skutecznych rezultatów, a w perspektywie długoterminowej, przyczynienie się do osiągnięcia celów organizacji w zakresie bezpieczeństwa.

6.5.3 Dobre podejmowanie decyzji nie jest łatwe. Decyzje są często podejmowane bez możliwości uwzględnienia wszystkich istotnych czynników. Decydenci mogą również wykazywać stronniczość, która, świadomie lub nie, wpływa na podejmowane decyzje.

6.5.4 Intencja D3M niekoniecznie polega na podejmowaniu perfekcyjnej lub idealnej decyzji, ale raczej na podejmowaniu dobrej decyzji, która osiągnie cel krótkoterminowy (co do którego podejmuje się rzeczywistą

decyzję) i działa w kierunku zaspokojenia celu długoterminowego (poprawa poziomu bezpieczeństwa organizacji). Dobre decyzje spełniają następujące kryteria i są:

- a) *Przejrzyste*: społeczność lotnicza powinna znać wszystkie czynniki, które wpływają na decyzję, w tym proces zastosowany do wypracowania decyzji.
- b) *Odpowiedzialne*: decydent „jest właścicielem” decyzji i związanych z nią wyników. Klarowność i przejrzystość niesie ze sobą również odpowiedzialność – nie jest łatwo ukryć się za decyzją, gdzie role i obowiązki są szczegółowo określone i gdzie oczekiwania związane z nową decyzją są wyraźnie zarysowane.
- c) *Uczciwe i obiektywne*: decydentowi nie podlega czynnikom, które nie są istotne (np. zysk pieniężny lub relacje osobiste).
- d) *Uzasadnione i możliwe do obrony*: decyzja może być uzasadniona, biorąc pod uwagę dane wejściowe do decyzji i realizowany proces.
- e) *Powtarzalne*: mając te same informacje, które były dostępne dla osoby podejmującej decyzję, i przy użyciu tego samego procesu, inna osoba wypracuje taką samą decyzję.
- f) *Wykonywalne*: decyzja jest wystarczająco jasna, a klarowność ogranicza niepewność do minimum.
- g) *Pragmatyczne*: ludzie są stworzeniami pełnymi emocji, co oznacza, że wyeliminowanie emocji z decyzji jest niewykonalne. Jednak to, co można wyeliminować, to samolubne uprzedzenia emocjonalne. Pytanie, które należy zadać w obliczu trudnych decyzji to: komu decyzja ma służyć?

6.5.5 Zalety podejmowania decyzji w oparciu o dane

6.5.5.1 D3M umożliwia decydentom skupienie się na pożądanym wyniku bezpieczeństwa, które są zgodne z polityką i celami w zakresie bezpieczeństwa, i które odnoszą się do różnych aspektów związanych z zarządzaniem zmianą, ocenami ryzyka bezpieczeństwa, itp. D3M może pomóc w podejmowaniu decyzji związanych z:

- a) zmianami, których można oczekiwać w wymaganiach ustawowych i regulacyjnych, nowych technologiach lub zasobach, które mogą mieć wpływ na organizację;
- b) potencjalnymi zmianami potrzeb i oczekiwań społeczności lotniczej i zainteresowanych stron;
- c) różnymi priorytetami, które należy ustalić i którymi należy zarządzać (np. strategiczne, operacyjne, dotyczące zasobów);
- d) nowymi umiejętnościami, kompetencjami, narzędziami, a nawet procesami zarządzania zmianą, które mogą być potrzebne do wdrożenia nowych decyzji;
- e) ryzykami, które muszą być oceniane, zarządzane i ograniczane do minimum;
- f) istniejącymi usługami, produktami i procesami, które obecnie stanowią największą wartość dla zainteresowanych stron; oraz
- g) ewoluującym zapotrzebowaniem na nowe usługi, produkty i procesy.

6.5.5.2 Ustrukturyzowane podejście, takie jak D3M, prowadzi decydentów do podejmowania decyzji zgodnych z danymi dotyczącymi bezpieczeństwa. Wymaga to zaufania do struktury zarządzania poziomem bezpieczeństwa; jeżeli istnieje zaufanie do systemu SDCPS, będzie istnieć zaufanie do wszelkich decyzji z niego wynikających.

6.5.6 Wyzwania związane z podejmowaniem decyzji w oparciu o dane

6.5.6.1 Wdrożenie procesów zbierania i analizy danych wymaga czasu i pieniędzy, a także wiedzy i umiejętności, które mogą nie być łatwo dostępne dla organizacji. Odpowiednia ilość czasu i zasobów przydzielona na proces podejmowania decyzji musi być dokładnie przemyślana. Czynniki, które należy wziąć pod uwagę, obejmują ilość pieniędzy zaangażowanych w daną decyzję, obszar oddziaływania decyzji i jej wpływ na bezpieczeństwo. Jeżeli organizacja nie rozumie zakresu zaangażowania, proces D3M może stać się źródłem frustracji dla decydentów ds. bezpieczeństwa, powodując, że podważają jego wartość lub zaprzestają jego realizacji. Podobnie jak krajowy program bezpieczeństwa i system zarządzania bezpieczeństwem, proces D3M i zarządzanie poziomem bezpieczeństwa wymagają zobowiązania do budowania i podtrzymywania struktur i umiejętności niezbędnych do uzyskania jak największych możliwości oferowanych przez D3M.

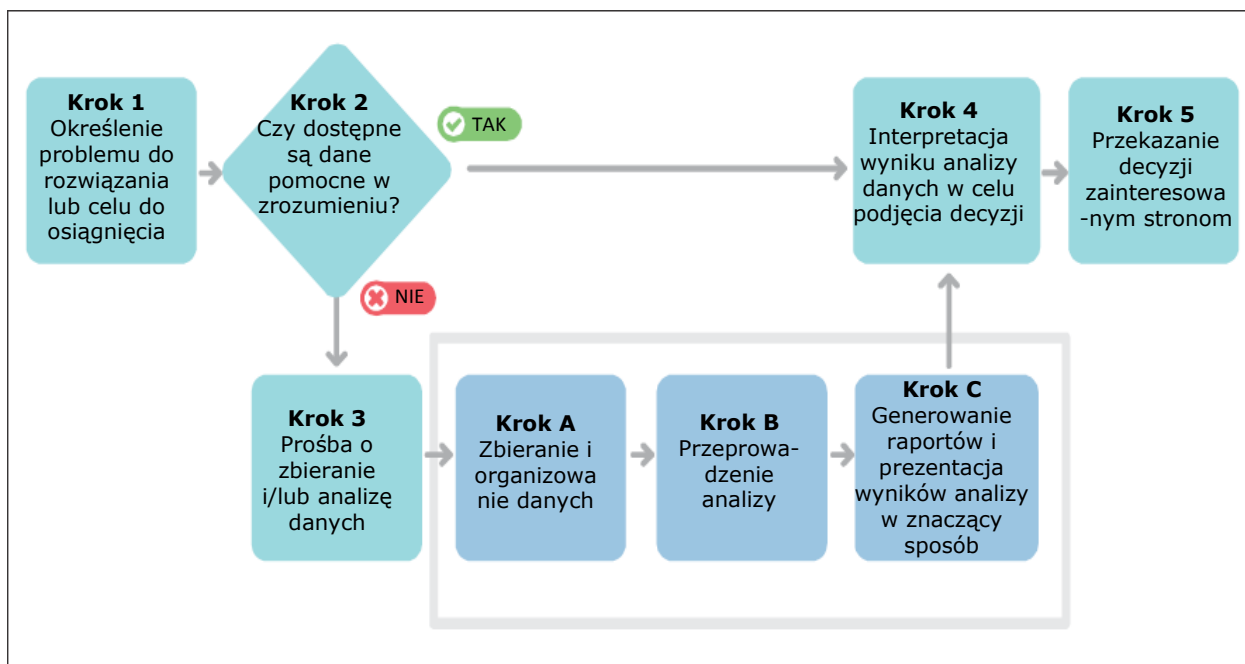
6.5.6.2 Trudniej jest zbudować zaufanie do danych aniżeli zaufać danym wejściowym i opinii eksperta. Przyjęcie podejścia D3M wymaga zmiany kultury i sposobu myślenia organizacji, gdzie decyzje opierają się na wiarygodnych wskaźnikach SPI i wynikach innych analiz danych bezpieczeństwa.

6.5.6.3 W niektórych przypadkach proces podejmowania decyzji może zostać spowolniony z powodu poszukiwania „najlepszego możliwego” rozwiązania, co określane jest również mianem „paraliżu analizy”. Strategie, których można użyć, aby tego uniknąć, obejmują:

- a) ustalenie terminu;
- b) posiadanie dobrze zdefiniowanego zakresu i celu; oraz
- c) niedążenie do „perfekcyjnej” decyzji lub rozwiązania za pierwszym razem, ale wypracowanie „odpowiedniej” i „praktycznej” decyzji oraz doskonalenie kolejnych decyzji.

6.5.7 Proces podejmowania decyzji w oparciu o dane

6.5.7.1 Proces D3M może stanowić narzędzie o krytycznym znaczeniu zwiększającym wartość i skuteczność programu SSP i systemu SMS. Skuteczne zarządzanie bezpieczeństwem zależy od podejmowania uzasadnionych i świadomych decyzji. Z kolei efektywny proces D3M opiera się na jasno określonych wymaganiach w zakresie danych i informacji bezpieczeństwa, standardów, metod zbierania danych, zarządzania danymi, analizy i udostępniania, spośród których wszystkie są elementami składowymi procesu D3M. Rysunek 6-3 przedstawia proces D3M.



Rysunek 6-3. Fazy podejmowania decyzji w oparciu o dane

Krok 1 – Określenie problemu lub celu

6.5.7.2 Pierwszym krokiem w planowaniu i ustanowieniu procesu D3M jest określenie problemu, który musi być rozwiązany lub celu w zakresie bezpieczeństwa, który musi zostać osiągnięty. Na jakie pytanie należy odpowiedzieć? Jaką decyzję muszą podjąć osoby podejmujące decyzje dotyczące bezpieczeństwa? W jaki sposób dostosuje się do bardziej strategicznych celów organizacyjnych? W procesie definiowania problemu decydenci powinni zadać sobie następujące pytania:

- Czy zbieranie i analiza danych wspierają i odnoszą się do celów w zakresie bezpieczeństwa organizacji lub do szczegółowych celów bezpieczeństwa?
- Czy wymagane dane są dostępne? Lub czy można go uzyskać w rozsądny sposób?
- Czy zbieranie i analizowanie danych jest praktyczne i wykonalne?
- Czy dostępne są wymagane zasoby (ludzie, sprzęt, oprogramowanie, fundusze)?

6.5.7.3 W kontekście zarządzania bezpieczeństwem, główne problemy występujące w organizacji są związane z oceną i wyborem priorytetów bezpieczeństwa – zgodnie z celami w zakresie bezpieczeństwa - i ustanowieniem środków łagodzących ryzyko bezpieczeństwa.

Krok 2 – Dostęp do danych w celu wsparcia procesu podejmowania decyzji

6.5.7.4 Następnym krokiem jest określenie, jakie dane są potrzebne do rozwiązania problemu (z uwzględnieniem przepisów w sprawie ochrony informacji). Żadne dane nie są bardziej wartościowe niż inne dane. Należy skupić się na tym, czy dostępne dane są odpowiednie w celu rozwiązania problemu. Jeżeli wymagane dane są dostępne, należy przejść do kroku 4. Jeżeli właściwe dane nie są dostępne, organizacja będzie musiała zbierać, przechowywać, analizować i prezentować nowe dane bezpieczeństwa i informacje bezpieczeństwa w znaczący sposób.

Krok 3 - Prośba o dane w celu wsparcia procesu podejmowania decyzji

6.5.7.5 Jeżeli dane nie są dostępne, organizacja musi znaleźć sposoby ich zbierania. Może to oznaczać ustanowienie innego wskaźnika SPI i być może powiązanego z nim poziomu SPT. Ustanowienie dodatkowych wskaźników może być kosztowne. Po oszacowaniu kosztów organizacja powinna ocenić, czy korzyści przewyższają koszty. Należy skupić się przede wszystkim na identyfikacji, monitorowaniu i pomiarze danych bezpieczeństwa, które są potrzebne do podejmowania skutecznych decyzji dotyczących bezpieczeństwa w oparciu o dane. Jeżeli koszty przewyższają korzyści, należy rozważyć alternatywne źródła danych i/lub wskaźniki.

6.5.7.6 W fazie planowania procesu D3M organizacja musi zdefiniować co chce osiągnąć poprzez ustanowienie SPT i SPI oraz poprzez analizę danych. Dlaczego organizacja musi rozwiązać zidentyfikowany problem? Jaki jest rozsądny cel? Oraz jak i gdzie decydenci ds. bezpieczeństwa wykorzystają wyniki zbierania i analizy danych? Jednoznaczne rozumienie przyczyn, dla których organizacja musi zbierać, analizować, udostępniać i wymieniać dane i informacje bezpieczeństwa, ma fundamentalne znaczenie dla każdego systemu SDCPS.

6.5.7.7 Aby umożliwić organizacji identyfikację trendów, podejmowanie świadomych decyzji, ocenę poziomu bezpieczeństwa w odniesieniu do zdefiniowanych celów, ocenę ryzyka lub spełnienie wymagań, połączeniu ulegają następujące elementy:

- a) zarządzanie poziomem bezpieczeństwa – w ramach opieki nad danymi bezpieczeństwa i informacjami bezpieczeństwa;
- b) system SDCPS – jako funkcja zbierania i przetwarzania danych bezpieczeństwa; oraz
- c) D3M jako niezawodny proces decyzyjny.

Krok 4 – Interpretacja wyników analizy danych i podejmowanie decyzji w oparciu o dane

6.5.7.8 Zebrane dane muszą być przedstawione decydentom we właściwym czasie i w znaczący sposób. Odpowiedniość i rozmiar zbiorów danych, stopień zaawansowania analiz i umiejętności analityków danych będą skuteczne tylko wtedy, kiedy dane będą prezentowane kiedy zajdzie taka potrzeba oraz w formatach, które ułatwiają decydentom zrozumienie. Spostrzeżenia uzyskane na podstawie danych powinny stanowić źródło informacji przy podejmowaniu decyzji, a w konsekwencji, przyczyniać się do poprawy poziomu bezpieczeństwa.

6.5.7.9 Dostępnych jest wiele modeli decyzyjnych. Zastosowanie uzgodnionego i znormalizowanego podejścia zwiększy do maksimum spójność i skuteczność decyzji organizacji podejmowanych w oparciu o dane. Większość z nich obejmuje następujące kroki:

- a) zebranie zespołu/grupy z niezbędnymi umiejętnościami i doświadczeniem (np. grupa ds. działań związanych z bezpieczeństwem (SAG));
- b) jasne zdefiniowanie problemu lub celu w zakresie bezpieczeństwa oraz kontekstu;
- c) przegląd SPT organizacji i celów w zakresie bezpieczeństwa dla zapewnienia ciągłej zgodności;
- d) przegląd i interpretacja danych dotyczących bezpieczeństwa w celu zrozumienia czego dotyczą;
- e) uwzględnienie i analiza realnych alternatyw;
- f) uwzględnienie ryzyka działań (lub zaniechań);
- g) uzyskanie konsensusu wśród grupy decyzyjnej;

- h) zobowiązanie do podejmowania decyzji w oparciu o dane i realizacja działań w oparciu o decyzje (zamiana słów w czyny); oraz
- i) monitorowanie i ocena wyników.

Krok 5 – Przekazanie decyzji

6.5.7.10 Aby decyzja dotycząca bezpieczeństwa była skuteczna, należy ją przekazać zainteresowanym stronom, w tym:

- a) personelowi, od którego wymaga się podjęcia niezbędnych działań;
- b) osobie, która zgłosiła sytuację (jeżeli jest to wymagane);
- c) całemu personelowi, w celu zapewnienia, że jest on informowany o ulepszeniach w zakresie bezpieczeństwa (promocja bezpieczeństwa: Państwa odnoszą się do Rozdziału 8; podmioty prowadzące działalność w lotnictwie cywilnym odnoszą się do Rozdziału 9); oraz
- d) menedżerom, w celu zapewnienia, że decyzja dotycząca bezpieczeństwa jest włączona w proces uczenia się organizacji.

6.5.7.11 Więcej informacji na temat komunikacji w zakresie bezpieczeństwa: pkt 8.6 dla Państw i pkt 9.6 dla podmiotów prowadzących działalność w lotnictwie cywilnym.

ROZDZIAŁ 7

OCHRONA DANYCH BEZPIECZEŃSTWA, INFORMACJI BEZPIECZEŃSTWA I POWIĄZANYCH ŹRÓDEŁ

7.1. CELE I TREŚĆ

7.1.1 Niniejszy rozdział opisuje podstawowe zasady regulujące ochronę danych bezpieczeństwa oraz informacji bezpieczeństwa uzyskanych lub pochodzących z systemów zgłaszania zdarzeń dotyczących bezpieczeństwa, a także źródła takich danych i informacji.¹ Zawiera również wytyczne i porady dotyczące wdrażania tych zasad przez krajowe organy lotnicze, podmioty lotnicze, prawodawców, prawników, prokuratorów, urzędników sądowych i inne właściwe organy odpowiedzialne za podejmowanie decyzji dotyczących wykorzystania i ochrony danych bezpieczeństwa, informacji bezpieczeństwa i związanych z nimi źródeł. Niniejszy rozdział może być przydatny dla wszystkich innych osób, które chcą uzyskać dostęp do danych bezpieczeństwa lub informacji bezpieczeństwa lub poszukują możliwości ich ujawnienia.

7.1.2 Rozdział odnosi się do następujących tematów:

- a) podstawowe zasady;
- b) zakres i poziom ochrony;
- c) zasady ochrony;
- d) zasady stosowania wyjątków;
- e) upublicznianie;
- f) ochrona zarejestrowanych danych; oraz
- g) udostępnianie i wymiana informacji bezpieczeństwa.

7.2. PODSTAWOWE ZASADY

7.2.1 Celem ochrony danych bezpieczeństwa, informacji bezpieczeństwa i związanych z nimi źródeł jest zapewnienie ich ciągłej dostępności w celu wykorzystania do utrzymania lub poprawy bezpieczeństwa lotniczego, przy jednoczesnym zachęcaniu osób i organizacji do zgłaszania danych bezpieczeństwa i informacji bezpieczeństwa. W tym kontekście, znaczenie wdrażania zabezpieczeń nie może być zawyżone. Zabezpieczenia nie mają na celu zwolnienia źródeł z ich obowiązków związanych z bezpieczeństwem lub ingerowania we właściwe zarządzanie wymiarem sprawiedliwości.

7.2.2 Bezpieczeństwo lotnicze nie jest wyłączną odpowiedzialnością Państw lub podmiotów lotniczych. Jest to wspólna odpowiedzialność, do której powinny przyczyniać się wszystkie zainteresowane strony, między innymi, poprzez dostarczanie odpowiednich danych i informacji za pomocą zgłoszeń zdarzeń związanych z bezpieczeństwem.

¹ Zgodnie z Załącznikiem 19, źródła danych dotyczących bezpieczeństwa i informacji dotyczących bezpieczeństwa obejmują zarówno osoby fizyczne jak i organizacje.

7.2.3 Chociaż dane i informacje mogą pochodzić z różnych źródeł, zgłaszanie danych bezpieczeństwa i informacji bezpieczeństwa przez osoby i organizacje w systemie lotniczym ma fundamentalne znaczenie dla zarządzania bezpieczeństwem. Skuteczne systemy zgłaszania pomagają zapewnić, że ludzie chcą zgłaszać swoje błędy i doświadczenia, co umożliwia Państwu i podmiotom lotniczym dostęp do odpowiednich danych i informacji niezbędnych do rozwiązania istniejących i potencjalnych braków i zagrożeń dotyczących bezpieczeństwa. Jest to możliwe dzięki stworzeniu środowiska, w którym ludzie mogą być pewni, że dane bezpieczeństwa i informacje bezpieczeństwa będą wykorzystywane wyłącznie do utrzymania i poprawy bezpieczeństwa, chyba że zastosowanie ma jedna z zasad stosowania wyjątków.

7.2.4 Załącznik 19 nie zapewnia ochrony osobom fizycznym lub organizacjom wymienionym w zgłoszeniu. Państwa mogą jednak rozszerzyć ochronę na osoby lub organizacje wymienione w zgłoszeniu.

7.2.5 Ważne jest, aby chronione były zarówno osoby fizyczne, jak i organizacje, jak również dane bezpieczeństwa i informacje o bezpieczeństwie, które są przez nie zgłaszane. Osoby i organizacje są chronione poprzez:

- a) zapewnienie, że nie zostaną ukarane na podstawie złożonego przez nie zgłoszenia; oraz
- b) ograniczenie wykorzystania zgłaszanych danych bezpieczeństwa i informacji bezpieczeństwa do celów utrzymania lub poprawy bezpieczeństwa.

Zabezpieczenia te mają zastosowanie, chyba że obowiązuje jedna z zasad stosowania wyjątków omówionych poniżej.

7.2.6 Załącznik 19 wymaga od Państw zapewnienia, że dane bezpieczeństwa i informacje bezpieczeństwa nie są wykorzystywane do celów innych niż określone w **zasadach ochrony**, chyba że zastosowanie ma zasada stosowania wyjątków. **Zasady stosowania wyjątków** określają okoliczności, w których może być dopuszczalne odstępstwo od tych zasad ochrony.

7.2.7 Działania zapobiegawcze, naprawcze lub zaradcze mogą być podejmowane przez Państwa i podmioty lotnicze na podstawie zgłoszonych danych bezpieczeństwa i informacji bezpieczeństwa w celu utrzymania lub poprawy bezpieczeństwa, to znaczy, w celu umożliwienia Państwu i podmiotom lotniczym podjęcie odpowiednich kroków w celu:

- a) ochrony przed możliwością natychmiastowych szkód lub obrażeń w wyniku ryzyka bezpieczeństwa do momentu jego identyfikacji i złagodzenia;
- b) zapewnienia, że podjęto odpowiednie działania w celu ograniczenia do minimum prawdopodobieństwa ponownego wystąpienia takiego ryzyka w przyszłości;
- c) zapobiegania narażeniu na ryzyko bezpieczeństwa, które nie zostało złagodzone; lub
- d) zapewnienia integralności samego systemu zgłaszania oraz większego systemu, którego system zgłaszania jest częścią.

7.2.8 Ponieważ takie działania mają fundamentalne znaczenie dla celów i skuteczności każdego systemu zarządzania bezpieczeństwem, Załącznik 19 wyraźnie stanowi, że Państwa nie mają zakazu podejmowania działań zapobiegawczych, naprawczych lub zaradczych w celu utrzymania lub poprawy bezpieczeństwa lotniczego. Działania takie mogą być podejmowane jako funkcja mających zastosowanie procesów zarządzania bezpieczeństwem i dlatego nie podlegają zasadom stosowania wyjątków, o których mowa w Załączniku 19.

7.2.9 Działania zapobiegawcze, naprawcze lub zaradcze mogą pociągać za sobą ograniczenie lub zapobieganie² wykonywania określonych przywilejów³, świadczenia usług lub eksploatacji statków powietrznych do czasu skutecznego rozstrzygnięcia zidentyfikowanych ryzyk bezpieczeństwa. Podejmowane w tym celu, zgodnie z ustalonymi procedurami, działania ochronne lub zapobiegawcze nie mogą być uważane za sankcje karne lub dyscyplinarne. Celem takich działań jest zapobieganie lub minimalizowanie narażenia na działanie nieograniczonego ryzyka bezpieczeństwa.

7.2.10 Zasady dotyczące ochrony danych bezpieczeństwa i informacji bezpieczeństwa oraz ich źródeł, o których mowa w Załączniku 19, zapewniają większą jasność i przejrzystość, a także równe szanse, w celu ułatwienia wymiany danych bezpieczeństwa oraz informacji bezpieczeństwa pomiędzy Państwami, zgodnie z wymogami Załącznika 19

7.3. ZAKRES OCHRONY

7.3.1 Zakres danych bezpieczeństwa i informacji bezpieczeństwa objętych zasadami ochrony

7.3.1.1 Ochrona ma zastosowanie do danych bezpieczeństwa i informacji bezpieczeństwa zgromadzonych i pochodzących z dobrowolnego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa i powiązanych źródeł. Może ona mieć zastosowanie do obowiązkowych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa w stosownych przypadkach (patrz pkt 7.4.3 poniżej). Źródłami danych bezpieczeństwa i informacji bezpieczeństwa mogą być osoby fizyczne lub organizacje.

7.3.1.2 W niektórych Państwach systemy zgłaszania zdarzeń dotyczących bezpieczeństwa mogą obejmować zgłaszanie danych na potrzeby badań bezpieczeństwa przez organy Państwa lub podmioty lotnicze, danych i informacji uzyskanych w ramach ogólnodostępnych systemów zgłaszania (w tym automatycznych oraz manualnych systemów zbierania danych) lub innych istotnych danych i informacji dotyczących bezpieczeństwa. Zasady ochrony i zasady stosowania wyjątków mogą zatem zostać rozszerzone na dane bezpieczeństwa i informacje bezpieczeństwa uzyskane również przez te systemy.

7.3.1.3 Istnieją inne przypadki, w których mają zastosowanie zasady ochrony i zasady stosowania wyjątków. Na przykład Załącznik 6 - *Eksploatacja statków powietrznych, Część I - Międzynarodowy zarobkowy transport lotniczy - Samoloty* stanowi, że źródła programów analizy danych o locie (FDA) powinny być chronione zgodnie z zasadami zawartymi w Załączniku 19.

7.3.1.4 Rodzaj danych bezpieczeństwa i informacji bezpieczeństwa, które mogą zostać uzyskane, jak również rodzaje systemów, które mogą być częścią systemów zgłaszania zdarzeń dotyczących bezpieczeństwa mogą ewoluować wraz z rozwojem systemów zarządzania bezpieczeństwem. Dane bezpieczeństwa, informacje bezpieczeństwa i systemy zgłaszania zdarzeń dotyczących bezpieczeństwa, które nie zostały wyraźnie określone w Załączniku 19 na obecnym etapie, mogą podlegać przepisom Załącznika 19 w przyszłości.

7.3.2 Interakcja z zasadami ochrony zawartymi w innych Załącznikach

7.3.2.1 Niektóre rodzaje danych bezpieczeństwa i informacji bezpieczeństwa, które są chronione na mocy Załącznika 19, mogą w pewnych okolicznościach podlegać innym wymogom ochrony.

² Zapobieganie wykorzystywaniu przywilejów może obejmować zawieszenie lub cofnięcie przywilejów wynikających z licencji.

³ Przywileje posiadacza upoważnienia są określone w licencji lub certyfikacie wydanym przez władze lotnicze Państwa.

7.3.2.2 Załącznik 19 określa, że w przypadku wszczęcia badania zgodnie z Załącznikiem 13, rejestry dotyczące badań wypadków i incydentów, o których mowa w Załączniku 13, podlegają ochronie określonej w Załączniku 13, a nie w Załączniku 19.

7.3.2.3 Zasada ta obowiązuje od momentu wystąpienia wypadku lub incydentu zgodnie z Załącznikiem 13 i pozostaje w mocy nawet po opublikowaniu raportu końcowego. Wytyczne w zakresie ochrony danych z badań wypadków i incydentów znajdują się w *Podręczniku ochrony informacji dotyczących bezpieczeństwa* (Doc 10053).

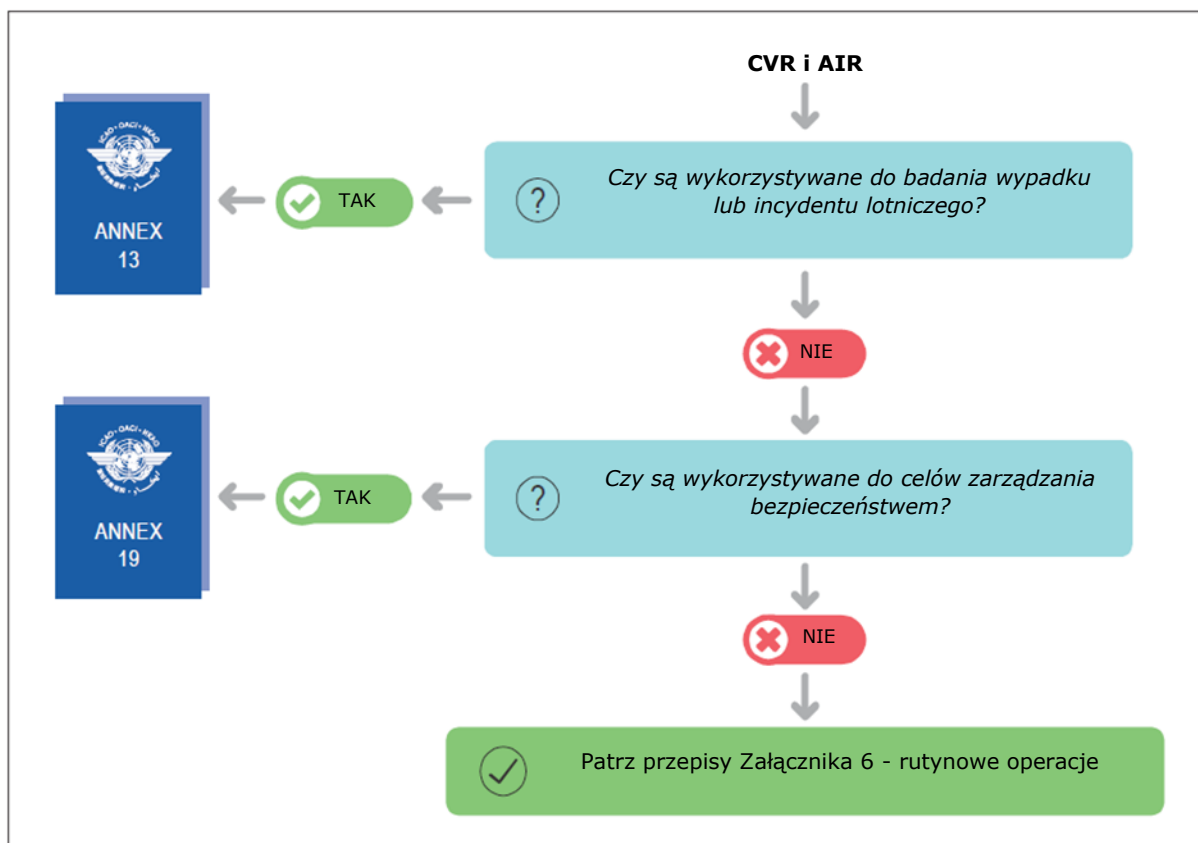
7.3.2.4 Podobnie, podczas gdy Załącznik 19 zapewnia ochronę zarejestrowanych danych w sytuacji kiedy są one wykorzystywane do celów zarządzania bezpieczeństwem, Załącznik 6 zapewnia ochronę zapisów rejestratora parametrów lotu podczas normalnej pracy, poza badaniami będącymi w zakresie Załącznika 13.

7.3.2.5 Załącznik 6 odnosi się do stosowania pokładowych rejestratorów rozmów w kabinie pilota (CVR) i rejestratorów obrazu w powietrzu (AIR), które powinno być ograniczone do celów związanych z bezpieczeństwem, z odpowiednimi zabezpieczeniami do inspekcji systemów rejestratora parametrów lotu lub kiedy poszukiwane są powiązane nagrania lub skrypty dla celów postępowań karnych. Takie postępowania karne wprowadza się do zmiany jako wyjątek od zasad ochrony przyznanych CVR i AIR w celu umożliwienia właściwym organom dostępu i korzystania z tego typu nagrań i ich skryptów bez ograniczeń w przypadkach, w których popełniane są przestępstwa, a zaangażowani członkowie załogi mogą nie wyrażać zgody na takie wykorzystanie (np. przypadki porwania).

7.3.2.6 Podobnie, stosowanie rejestratorów parametrów lotu (FDR), systemów rejestracji danych statków powietrznych (ADRS), a także AIR klasy B i C oraz systemów rejestracji obrazu w powietrzu (AIRS) powinno być ograniczone do celów zdatności do lotu lub obsługi technicznej, w tym programy FDA, z odpowiednimi zabezpieczeniami zgodnie z Załącznikiem 19.

7.3.2.7 Rysunek 7-1 przedstawia ogólne wytyczne dotyczące interakcji pomiędzy schematami ochrony, o których mowa w Załączniku 6, 13 i 19, i należy je stosować zgodnie z obowiązującymi przepisami.

7.3.2.8 W odniesieniu do programów analizy danych o locie (FDA), źródła są w każdej sytuacji chronione zgodnie z zasadami zawartymi w Załączniku 19.



Rysunek 7-1. Wytyczne w zakresie interakcji przepisów dotyczących ochrony

7.3.3 Zastosowanie zasad określonych w Załączniku 19 do podmiotów lotniczych

7.3.3.1 Załącznik 19 opisuje środowisko zgłaszania zdarzeń, które sprzyja zaufaniu jako środowisku „gdzie pracownicy i personel operacyjny mogą ufać, że ich działania lub zaniechania współmierne do ich szkolenia i doświadczenia nie będą karane”. Działanie lub zaniechanie jest współmierne do szkolenia i doświadczenia danej osoby, jeżeli można przewidzieć, że osoba o tym samym poziomie doświadczenia i szkolenia może zrobić to samo lub nie. Takie środowisko ma fundamentalne znaczenie dla skutecznego i wydajnego zgłaszania zdarzeń dotyczących bezpieczeństwa.

7.3.3.2 Zachęcanie ludzi do zgłaszania odpowiednich danych bezpieczeństwa lub informacji bezpieczeństwa wymaga, aby źródła tych zgłoszeń były chronione przed działaniami podejmowanymi przez Państwo zgodnie z Załącznikiem 19, jak również przed działaniami podejmowanymi w ich środowisku pracy.

7.3.3.3 Przepisy Załącznika mają na celu zapewnienie minimalnych wymagań, które muszą spełniać wszystkie Państwa, niezależnie od wielkości i złożoności działalności lotnictwa cywilnego. Poszczególne Państwa są odpowiedzialne za opracowanie wymogów wystarczających do zapewnienia zadowalającej zgodności ze strony Państwa i jego podmiotów prowadzących działalność w lotnictwie cywilnym.

7.3.3.4 Zasady ochrony i zasady stosowania wyjątków mające zastosowanie do danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł, o których mowa w Załączniku 19, powinny być wdrażane zarówno przez Państwa, jak i przez podmioty lotnicze. Aby zapewnić osiągnięcie tego celu, od Państw oczekuje się przyjęcia odpowiednich krajowych przepisów ustawowych, wykonawczych i politycznych, w celu zapewnienia, że podmioty lotnicze wdrażają przepisy zawarte w Załączniku 19.

7.4. POZIOM OCHRONY

7.4.1 Warunki kwalifikujące do ochrony zgodnie z Załącznikiem 19

7.4.1.1 Załącznik 19 wymaga od Państw określenia warunków, zgodnie z którymi dane bezpieczeństwa i informacje bezpieczeństwa kwalifikują się do ochrony. W ten sposób od Państw oczekuje się rozważenia, czy:

- a) dane bezpieczeństwa lub informacje bezpieczeństwa są objęte zakresem Załącznika 19;
- b) istnieją okoliczności, w których Załącznik 6 lub Załącznik 13 mają pierwszeństwo przed Załącznikiem 19; oraz
- c) zastosowanie ma zasada stosowania wyjątków.

7.4.2 Działania niezbędne do utrzymania lub poprawy bezpieczeństwa lotniczego

7.4.2.1 Załącznik 19 zapewnia, że Państwowi i podmiotom lotniczym nie uniemożliwia się wykorzystywanie danych bezpieczeństwa lub informacji bezpieczeństwa w celu podjęcia działań zapobiegawczych, naprawczych lub zaradczych, które są niezbędne do utrzymania lub poprawy bezpieczeństwa lotniczego. Zgodnie z tym celem, takie działania, jeżeli zostały podjęte, powinny, w miarę możliwości, unikać finansowych, wizerunkowych lub innych niekorzystnych skutków w stosunku do źródła danych bezpieczeństwa lub informacji bezpieczeństwa.

7.4.2.2 Działania zapobiegawcze, naprawcze lub zaradcze mają na celu odniesienie się do okoliczności lub warunków stanowiących nieakceptowalne ryzyko bezpieczeństwa lotniczego.

7.4.2.3 *Działanie zapobiegawcze* może być rozumiane jako działanie podejmowane w celu zapobieżenia wystąpieniu lub ponownemu wystąpieniu zdarzenia lub zagrożenia, które stanowi ryzyko bezpieczeństwa.

7.4.2.4 *Działanie naprawcze* może być rozumiane jako działanie podejmowane w celu rozwiązania określonych niedociągnięć lub braków związanych z bezpieczeństwem, takich jak np. posiadacz upoważnienia, który nie jest w stanie wykazać zgodności z obowiązującymi normami w zakresie bezpieczeństwa lub kompetencji. Konieczne może być podjęcie działań naprawczych w celu przywrócenia zgodności posiadacza upoważnienia.

7.4.2.5 *Działanie zaradcze* może być rozumiane jako działanie podejmowane w celu zaradzenia przyczynom szczególnych niedociągnięć lub braków związanych z bezpieczeństwem, takich jak szkolenia. Działanie zaradcze może również obejmować ograniczenie, zawieszenie lub cofnięcie przywilejów posiadacza upoważnienia, certyfikatu lub licencji, który nie spełnia wymogów niezbędnych do korzystania z tych przywilejów.

7.4.2.6 Chociaż działania takie mogą być określone jako służące jednemu lub innemu celowi, mogą one służyć więcej niż jednemu celowi. Na przykład, właściwy organ lub podmiot lotniczy może podjąć działania polegające na żądaniu od posiadacza licencji lub certyfikatu podjęcia dodatkowego szkolenia i powstrzymaniu się od korzystania z przywilejów wynikających z licencji lub certyfikatu do czasu pomyślnego ukończenia szkolenia. Właściwy organ może również podjąć działania mające na celu cofnięcie, usunięcie lub zawieszenie niektórych przywilejów certyfikatu organizacji. Takie działania, chociaż zaradcze, ponieważ dotyczą podstawowej przyczyny problemu związanego z bezpieczeństwem, mogą również zostać uznane za naprawcze, ponieważ dotyczą konkretnego braku. Niezależnie od charakteru podjętych działań, powinien istnieć jasny i możliwy do wykazania związek pomiędzy konkretnym podejmowanym działaniem a utrzymaniem lub poprawą bezpieczeństwa.

7.4.2.7 Dane bezpieczeństwa lub informacje bezpieczeństwa mogą ujawnić zagrożenia lub braki, które wymagają podjęcia działań zaradczych lub naprawczych w celu utrzymania bezpieczeństwa lub określenia obszarów, w których działania zapobiegawcze zwiększyłyby bezpieczeństwo lotnicze poprzez przeciwdziałanie potencjalnym lub pojawiającym się ryzykom. Aby określić stan lub zagrożenie uzasadniające podjęcie działań zapobiegawczych, naprawczych lub zaradczych, Państwa będą musiały korzystać z danych bezpieczeństwa lub informacji bezpieczeństwa. Dla przykładu, dane bezpieczeństwa i informacje bezpieczeństwa mogą być konieczne do ustalenia podstaw dla działań administracyjnych związanych z licencją lub do spełnienia wymaganych obciążeń dowodowych. Lub też dane bezpieczeństwa i informacje bezpieczeństwa mogą być konieczne do ustalenia potrzeby dodatkowego szkolenia osoby licencjonowanej lub zmian w systemach operatora. Użycie danych lub informacji może być również konieczne w celu zapewnienia integralności i prawidłowego działania systemu zgłaszania, oraz większego systemu, którego system zgłaszania jest częścią.

7.4.2.8 W zależności od okoliczności, działania zapobiegawcze, naprawcze lub zaradcze, chociaż niezamierzone, mogą być postrzegane jako kara przez osobę lub podmiot będące przedmiotem takich działań. Rzeczywiście, niektórzy mogą postrzegać wszelkie działania związane z licencją podjęte w celu wyeliminowania braków kompetencyjnych jako karę, a nie jako działania niezbędne do skorygowania lub naprawienia ryzyka dla bezpieczeństwa.

7.4.2.9 Pomimo tych spostrzeżeń Załącznik 19 nie zakazuje Państwu korzystania z danych bezpieczeństwa i informacji bezpieczeństwa w celu wsparcia działań niezbędnych do utrzymania lub poprawy bezpieczeństwa lotniczego. W przypadku gdy konieczne są działania w celu utrzymania lub poprawy poziomu bezpieczeństwa lotniczego lub w celu zapobieżenia pogorszeniu bezpieczeństwa systemu lotniczego w krótkim lub w dłuższym okresie czasu, Państwa mogą wykorzystywać dane bezpieczeństwa lub informacje bezpieczeństwa w celu wsparcia tych działań, pod warunkiem że mają one wyraźny cel i skutek zapobiegawczy, naprawczy lub zaradczy. W takich przypadkach Państwa powinny rozważyć podjęcie niezbędnych środków w celu jasnego przekazania uzasadnienia podjętych działań, aby wykazać cel i ograniczyć do minimum negatywny wpływ na proces zgłaszania w przyszłości. Z drugiej strony, wykorzystanie danych dotyczących bezpieczeństwa i informacji dotyczących bezpieczeństwa do podejmowania działań, w których nie można wykazać, że służą jednemu lub więcej z powyższych celów, i które zamiast tego mogą wykazywać cel czysto karny lub dyscyplinarny, powinno być zakazane, chyba że zastosowanie ma jedna z zasad stosowania wyjątków.

7.4.3 Ochrona obowiązkowych systemów zgłaszania

7.4.3.1 Załącznik 19 określa różne wymagania dotyczące ochrony danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł uzyskanych w ramach dobrowolnego i obowiązkowego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa. Ochrona danych bezpieczeństwa i informacji bezpieczeństwa uzyskanych w ramach dobrowolnego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa jest Normą, co ma na celu zapewnienie ciągłej dostępności i większej jednolitości wśród Państw, natomiast w przypadku obowiązkowych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa zapewnienie takiej ochrony jest Zalecaną metodą postępowania.

7.4.3.2 W niektórych jurysdykcjach, dane bezpieczeństwa i informacje bezpieczeństwa uzyskiwane w ramach obowiązkowego i dobrowolnego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa podlegają różnym poziomom ochrony, oferując lepszą ochronę danych bezpieczeństwa i informacji bezpieczeństwa w systemach dobrowolnych w porównaniu z danymi bezpieczeństwa i informacjami bezpieczeństwa w systemach obowiązkowych. Rozróżnienie to można uzasadnić koniecznością zachęcania do dobrowolnego dostarczania danych dotyczących bezpieczeństwa lub informacji dotyczących bezpieczeństwa w sposób, który nie jest uważany za konieczny, jak ma to miejsce w przypadku obowiązkowego systemu zgłaszania.

7.4.3.3 Inne Państwa oferują ten sam wysoki poziom ochrony danych bezpieczeństwa i informacji bezpieczeństwa zarówno w obowiązkowych, jak i dobrowolnych systemach zgłaszania zdarzeń dotyczących bezpieczeństwa. Może to być uzasadnione stwierdzeniem, że zgłaszanie wymagane przepisami prawa nie może samo w sobie być wystarczające do zapewnienia, że zgłaszane są odpowiednie dane bezpieczeństwa i informacje bezpieczeństwa, oraz że godne zaufania środowisko stanowi podstawą wszelkiego rodzaju zgłaszania. Rozszerzenie zabezpieczeń na obowiązkowe systemy zgłaszania może również zachęcić osoby zgłaszające do dostarczenia dodatkowych informacji, których w przeciwnym razie nie mogliby podać, gdyby zabezpieczenia te nie były dostępne.

7.4.3.4 Jeżeli Państwo rozszerza ochronę danych bezpieczeństwa i informacji bezpieczeństwa z dobrowolnych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa na systemy obowiązkowe, zasady ochrony oraz zasady stosowania wyjątków zawarte w Załączniku 19 powinny mieć zastosowanie do danych bezpieczeństwa i informacji bezpieczeństwa zgromadzonych przez obydwa te systemy, jak również do ich odpowiednich źródeł.

7.4.4 Ochrona danych i informacji w przestrzeni publicznej

7.4.4.1 Mogą wystąpić przypadki, w których dane bezpieczeństwa lub informacje bezpieczeństwa są dostępne w przestrzeni publicznej. W niektórych przypadkach może się zdarzyć, że takie dane bezpieczeństwa lub informacje bezpieczeństwa nie są wrażliwe, a ich dalsze ujawnienie nie wpłynie negatywnie na ciągłą dostępność danych bezpieczeństwa lub informacji bezpieczeństwa. Dane bezpieczeństwa i informacje bezpieczeństwa związane z pogodą mogą być przykładem takich niewrażliwych danych i informacji.

7.4.4.2 W innych przypadkach może zdarzyć się, że dane bezpieczeństwa i informacje bezpieczeństwa, zwykle podlegające zasadom ochrony, znajdują się w przestrzeni publicznej, na przykład, poprzez przeciek do mediów. W takich przypadkach Państwa powinny powstrzymać się od dalszego ujawniania danych i informacji, które wyciekły, ponieważ zasady ochrony nie zostaną automatycznie zniesione.

7.5. ZASADY OCHRONY

7.5.1 Zastosowanie zasad ochrony

7.5.1.1 Ochrona danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł powinna być domyślną pozycją Państwa. Państwo może zapewnić skuteczną ochronę prawną, popartą kompleksowymi i jasnymi procedurami.

7.5.1.2 Podstawowym celem ochrony jest zapewnienie ciągłej dostępności danych bezpieczeństwa i informacji bezpieczeństwa poprzez zachęcanie osób i organizacji do identyfikowania, zgłaszania, analizowania i korygowania braków. Wymaga to, aby wszystkie zaangażowane strony z wyprzedzeniem znały obowiązujące zasady i procesy ochrony. Takie zasady i procesy powinny zostać sformalizowane i nie powinny być otwarte na arbitralne zastosowania, jeżeli mają służyć jako podstawa systemu opartego na zaufaniu.

7.5.1.3 W ochronie danych bezpieczeństwa lub informacji bezpieczeństwa należy uwzględnić cel, jaki ochrona ma osiągnąć. Cel może wynikać z rodzaju danych i informacji, które mają być chronione. W wielu przypadkach ochrona ma na celu zapobieganie wykorzystywaniu danych bezpieczeństwa i informacji bezpieczeństwa w stosunku do osoby lub organizacji, która zgłosiła konkretne dane lub informacje. W innych przypadkach ważne może być zabezpieczenie danych bezpieczeństwa lub informacji bezpieczeństwa przed ogólną publikacją lub wykorzystaniem w kontekstach niezwiązanych z bezpieczeństwem, takich jak lokalne kontrowersje dotyczące użytkowania gruntów dotyczące eksploatacji lotnisk i kwestii redukcji hałasu.

7.5.1.4 Działania Państwa mają kluczowe znaczenie dla tworzenia przepisów ochronnych. W postępowaniu formalnym, w którym obowiązują zasady określające, jakie dowody mogą być przedstawiane, jedynie działanie Państwa może zapewnić niezbędną ochronę poprzez przyjęcie odpowiedniego ustawodawstwa lub przepisów, które albo zabraniają, albo ściśle ograniczają dopuszczalność chronionych informacji. Na przykład, w postępowaniu karnym przeciwko osobie, wykorzystanie dobrowolnego zgłoszenia złożonego przez oskarżonego powinno być zabronione, jeżeli nie jest bezpośrednio związane z domniemanym przestępstwem.

7.5.1.5 W postępowaniu cywilnym przeciwko podmiotowi lotniczemu, zasada powinna, co najmniej, wymagać domniemania wzruszalnego⁴, że informacje chronione nie mogą być wykorzystywane. W przypadku powództwa przeciwko przewoźnikowi lotniczemu za szkody poniesione w wyniku zdarzenia, powód może uzyskać ogólny dostęp do plików SMS operatora, w celu podjęcia próby odkrycia ogólnych informacji, które mogą nie być bezpośrednio związane z incydentem, ale które mogą mieć tendencję do przedstawienia operatora w niekorzystnym świetle. Ustalona procedura określania takich pytań powinna kierować właściwy organ (w tym przypadku najprawdopodobniej sąd), który ma za zadanie zastosowanie zasad stosowania wyjątków (omówionych bardziej szczegółowo w pkt 7.6), i wymagać od powoda dokładnego przedstawienia informacji, które mają być ujawnione oraz wykazać znaczenie informacji dla działania, a także wykazać niedostępność alternatywnych źródeł tych samych lub podobnych informacji. Właściwy organ może również zwrócić się do powoda z prośbą o wykazanie, w jaki sposób jest on poszkodowany poprzez brak dostępu do informacji. W przypadku decyzji o umożliwieniu takiego dostępu, właściwy organ powinien nałożyć formalne zabezpieczenia zgodnie z obowiązującymi wymogami proceduralnymi, takimi jak nakaz ochrony uniemożliwiający publikację i ograniczający dostęp do odpowiednich części postępowania.

7.5.1.6 W postępowaniu administracyjnym, w którym kwestionuje się szczególne kwalifikacje operacyjne lub techniczne, kompetencje i możliwości danej osoby lub organizacji, bezpieczeństwo prawie zawsze będzie stanowić problem. W takich przypadkach wymagane może być użycie danych bezpieczeństwa lub informacji bezpieczeństwa, ale egzekwowlane wymogi powinny przewidywać kontrolowane i ograniczone wykorzystanie takich danych i informacji. W przypadku gdy dane bezpieczeństwa lub informacje bezpieczeństwa stanowią podstawę decyzji w sprawach związanych z bezpieczeństwem, należy zachować szczególną ostrożność, aby zapobiec niekorzystnym lub szkodliwym konsekwencjom w stosunku do źródła informacji w wyniku wykorzystania wspomnianych danych i informacji. Generalnie, osoby i organizacje, które są zachęcane do zgłaszania w ramach chronionego systemu zgłaszania, uznają, że istnieją okoliczności, w których działania na rzecz bezpieczeństwa muszą być podejmowane w oparciu o, w całości lub w części, zgłoszenie podlegające ochronie. Egzekwowlane wymogi powinny zapewnić, że takie działanie jest zgodne z fundamentalną sprawiedliwością w dążeniu do utrzymania lub poprawy bezpieczeństwa.

7.5.1.7 Przykładem takiej sytuacji może być zgłoszenie kontrolera ruchu lotniczego, który stracił przytomność na krótki czas podczas pracy. Nie doszło do utraty separacji, a jedynym dowodem na to, że zdarzenie miało miejsce, było zgłoszenie kontrolera. Dla celów związanych z bezpieczeństwem analiza tego zgłoszenia wymagała dalszego badania, co z kolei wymagało, aby osoba zgłaszająca była możliwa do zidentyfikowania. Natychmiastowe działanie naprawcze może polegać na usunięciu kontrolera z czynnej służby (nie powodując niekorzystnych skutków finansowych lub wizerunkowych), przy jednoczesnym wykonaniu kompleksowych badań i przeglądu lekarskiego.

⁴ Domniemanie wzruszalne jest założeniem, które uznaje się za prawdziwe, chyba że zostanie ono obalone przez dowody.

Po ich zakończeniu, wynik może sprowadzać się do wydania orzeczenia lekarskiego, konieczności podjęcia leczenia lub przejścia na emeryturę (ponownie bez niekorzystnych skutków finansowych lub wizerunkowych). Gdyby kontroler został po prostu zwolniony, bardzo mało prawdopodobne jest, aby podobne zgłoszenia innych osób pojawiły się w przyszłości.

7.5.1.8 Do tego momentu koncentrowano się na bezpośrednich działaniach Państwa mających na celu zapewnienie niezbędnej i odpowiedniej ochrony. W praktyce większość danych bezpieczeństwa i informacji bezpieczeństwa, dla których wymagana jest ochrona, mieści się w środowisku operacyjnym podmiotu lotniczego i obejmuje relacje pomiędzy pracodawcami a pracownikami. Ochrona w takich sytuacjach nie zawsze może być przewidziana w prawodawstwie lub innych formach egzekwowalnych wymogów Państwa. Jednak nawet w takich przypadkach, Państwa mogą wymagać skutecznej ochrony poprzez procesy certyfikacji, zatwierdzania i ciągłego nadzoru. Załącznik 19 wymaga od określonych podmiotów lotniczych wdrożenia skutecznego systemu zarządzania bezpieczeństwem. Skuteczne zarządzanie bezpieczeństwem opiera się na gromadzeniu danych, analizie i ochronie. Bez danych system straciłby skuteczność. Krajowy program bezpieczeństwa powinien umożliwić Państwom kierowanie organizacjami w celu wdrożenia polityki zapewniającej ochronę swoich pracowników jako element ich systemów SMS.

7.5.1.9 Jednym ze sposobów zapewnienia takiej ochrony może być pozbawienie elementów pozwalających na identyfikację osoby zgłaszającej. Podczas gdy poufność zgłoszeń jest użyteczną strategią, całkowite pozbawienie elementów pozwalających na identyfikację, w miarę możliwości, eliminuje możliwość kontynuacji w fazie analizy. Polityki powinny koncentrować się na tym, jakiego zastosowania może dokonać właściwy organ, i na jakie może sobie pozwolić, z danymi bezpieczeństwa i informacjami bezpieczeństwa. Powyższa dyskusja (patrz pkt 7.5.1.6) w odniesieniu do postępowania administracyjnego ma również zastosowanie w kontekście pracodawca/pracownik. Po raz kolejny, osoby składające zgłoszenia w ramach systemu obowiązkowego będą je składać niechętnie, jeżeli zgłoszenia te lub inne dane zostaną wykorzystane do działań związanych z ukaraniem, zawieszeniem dyscyplinarnym lub zwolnieniem.

7.5.1.10 Gromadzenie danych bezpieczeństwa i informacji bezpieczeństwa za pomocą środków automatycznych, takich jak rejestratory FDR, rejestratory głosu lub wideo lub rejestratory środowiska ruchu lotniczego, powinno stanowić część każdej polityki lub regulacji w zakresie ochrony. Korzystanie z tych urządzeń w ramach gromadzenia danych SMS, jeżeli zezwalają na to regulacje lub polityka, musi być w pełni zgodne z zasadami ochrony w taki sam sposób jak ma to miejsce w przypadku dobrowolnie przekazywanych zgłoszeń. Zaufanie ze strony osób zgłaszających ma fundamentalne znaczenie dla skutecznego zarządzania bezpieczeństwem.

7.5.2 Postępowanie

7.5.2.1 Załącznik 19 wymaga od Państw zapewnienia, że dane bezpieczeństwa i informacje bezpieczeństwa nie są wykorzystywane w postępowaniach dyscyplinarnych, cywilnych, administracyjnych i karnych przeciwko pracownikom, personelowi operacyjnemu lub organizacjom, chyba że zastosowanie ma zasada stosowania wyjątków.

7.5.2.2 Termin „postępowanie” może być bardziej wszechstronny i szerszy niż termin „działanie”. Może również odnosić się do procesów danego organu w celu przeglądu lub egzekwowania „działań” podjętych przez inny organ (lub agencję w ramach tego samego organu). W ogólnym znaczeniu terminy „postępowanie” i „działanie” mogą być rozumiane jako obejmujące wszystkie podjęte kroki lub przyjęte środki mające na celu zainicjowanie, wdrożenie lub przegląd decyzji organu wpływającej na prawa, przywileje, interesy lub uzasadnione oczekiwania (ponieważ mogą one zostać określone na mocy obowiązujących przepisów). Z uwagi na różne systemy prawne, charakter i zakres poszczególnych działań lub postępowań może się różnić. Na przykład, w niektórych Państwach:

- a) *Działania lub postępowania karne i cywilne* zazwyczaj dotyczą organów sądowych. Postępowania te mogą obejmować rozpoczęcie działania, pojawienie się pozwanego, wszystkie dodatkowe lub tymczasowe kroki, pisma procesowe, procesy wykrywania i inne formalne zapytania. W wyniku takich działań lub postępowań, osoba może podlegać odszkodowaniu pieniężnemu, grzywnie lub w niektórych przypadkach karze więzienia.
- b) *Działania lub postępowania administracyjne* mogą obejmować zapytanie, badanie lub przesłuchanie przed organem regulacyjnym lub trybunałem, które odnosi się do działań mających na celu zmianę, zawieszenie, cofnięcie lub unieważnienie upoważnienia (dla ewidentnych celów związanych z bezpieczeństwem w niektórych przypadkach, a w innych przypadkach dla celów karnych).
- c) *Działania lub postępowania dyscyplinarne* mogą odnosić się do procesu, w którym pracodawca reaguje na rzeczywiste lub widoczne przypadki łamania lub naruszenia zasad i procedur przez pracownika. W wyniku takich działań lub postępowań pracownik może zostać uwolniony od domniemanego przewinienia, lub może zostać zdyscyplinowany lub zwolniony, jeżeli zarzuty są uzasadnione.

7.5.2.3 W wymienione powyżej działania i postępowania mogą być zaangażowane inne organy, takie jak sądy administracyjne, organy zawodowe, organy etyczne lub inne organy kontrolne w organizacji.

7.5.2.4 Ważne jest, aby pamiętać, że zasady ochrony nie mają zastosowania, kiedy Państwa podejmują działania zapobiegawcze, naprawcze lub zaradcze, które są niezbędne do utrzymania lub poprawy bezpieczeństwa lotniczego (patrz pkt 7.4.2 powyżej). Dotyczy to również każdego postępowania, działania lub środka związanego z działaniami zapobiegawczymi, naprawczymi lub zaradczymi podjętymi w celu utrzymania lub poprawy bezpieczeństwa. Na przykład wykorzystanie danych bezpieczeństwa lub informacji bezpieczeństwa w celu uzasadnienia podjęcia działania zapobiegawczego, naprawczego lub zaradczego jest dozwolone w postępowaniach wszczętych przez osobę lub organizację starającą się zakwestionować to działanie.

7.5.2.5 Chociaż mogą mieć miejsce przypadki, w których dane bezpieczeństwa lub informacje bezpieczeństwa są wykorzystywane w postępowaniach sądowych wszczętych przez stronę trzecią przeciwko źródłu zgłoszenia, zachęca się Państwa do podjęcia wszelkich niezbędnych środków w celu zapewnienia, że dane bezpieczeństwa i informacje bezpieczeństwa nie są wykorzystywane do celów innych niż utrzymanie lub poprawa bezpieczeństwa lotniczego (chyba że zastosowanie ma zasada stosowania wyjątków).

7.5.3 Wiarygodne zabezpieczenia

7.5.3.1 Niektóre czynniki mogą złagodzić negatywne konsekwencje związane z ujawnieniem lub wykorzystaniem danych bezpieczeństwa lub informacji bezpieczeństwa do celów innych niż utrzymanie lub poprawa bezpieczeństwa lotniczego. Ograniczenie wszelkich potencjalnych szkód wynikających z proponowanego ujawnienia lub wykorzystania może być możliwe poprzez wprowadzenie zabezpieczeń w celu dalszego ograniczenia w ujawnianiu lub wykorzystaniu danych bezpieczeństwa i informacji bezpieczeństwa. Państwo może włączyć do swojego ustawodawstwa lub przepisów, zgodnie z którymi uwzględniane jest zastosowanie zasad stosowania wyjątków, uprawnienia dla właściwego organu do nakładania wymogów zachowania tajemnicy w zakresie danych dotyczących bezpieczeństwa lub informacji dotyczących bezpieczeństwa po podjęciu decyzji zezwalającej na dostęp.

7.5.3.2 Pozbawienie elementów pozwalających na identyfikację źródła danych bezpieczeństwa i informacji bezpieczeństwa to kolejne zabezpieczenie, które może być używane przed ich ujawnieniem dla celów innych niż utrzymanie lub poprawa bezpieczeństwa lotniczego, na które zgodę wyraził właściwy organ. Pozbawienie elementów pozwalających na identyfikację może jednak być trudne w sytuacji kiedy źródła zapewniające dane bezpieczeństwa lub informacje bezpieczeństwa można łatwo ustalić na podstawie treści zgłoszonych danych lub informacji. Na przykład, zgłoszenie zdarzenia z udziałem typu statku powietrznego, który jest używany tylko przez jednego operatora w danej jurysdykcji może natychmiast wskazywać na tego operatora (lub nawet na pojedynczego pracownika) po prostu poprzez identyfikację typu statku powietrznego. W takich przypadkach, sposób oraz miejsce ujawnienia lub wykorzystania danych bezpieczeństwa lub informacji bezpieczeństwa, jak również charakter informacji, mają szczególne znaczenie.

7.5.3.3 Jeżeli dane bezpieczeństwa lub informacje bezpieczeństwa są proponowane do wykorzystania na forum, gdzie znajomość osób lub organizacji powiązanych z danymi lub informacjami jest ograniczona, wówczas właściwy organ może być pewien, że pozbawienie elementów pozwalających na identyfikację stanowi wystarczające zabezpieczenie źródeł. Podobnie, jeżeli charakter informacji jest przede wszystkim techniczny, w danych bezpieczeństwa lub informacjach bezpieczeństwa może nie być zbyt wiele elementów identyfikujących, które muszą być usunięte lub zredagowane, dzięki czemu zadanie zapewnienia ochrony jest łatwiejsze do osiągnięcia. Właściwy organ powinien również rozważyć czy forum proponowanego ujawnienia lub wykorzystania danych lub informacji oraz charakter informacji wpłynie na stopień, w jakim można zidentyfikować źródła, oraz czy usunięcie informacji identyfikujących będzie wystarczające. Jeżeli proponowane ujawnienie lub wykorzystanie może mieć negatywny wpływ na organizację lub firmę, taką jak operator statku powietrznego, wówczas właściwy organ powinien zdecydować, czy pozbawienie elementów pozwalających na identyfikację w danych lub informacjach zapewni ochronę podobną do tej, którą firma lub operator uzyskaliby, gdyby nie było zgody na ich ujawnienie lub wykorzystanie.

7.5.3.4 Jeżeli właściwy organ uzna, że pozbawienie elementów pozwalających na identyfikację w danych bezpieczeństwa i informacjach bezpieczeństwa może uniemożliwić planowane lub dopuszczalne wykorzystanie danych bezpieczeństwa lub informacji bezpieczeństwa, pozbawienie elementów pozwalających na identyfikację nie będzie właściwe. W związku z tym Państwa mogą zdecydować się na wdrożenie innego rodzaju zabezpieczeń (lub kombinacji zabezpieczeń), w celu umożliwienia ograniczonego ujawnienia w określonym celu, jednocześnie zapobiegając szerszemu wykorzystaniu lub upublicznieniu danych bezpieczeństwa lub informacji bezpieczeństwa. Nakazy ochronne, postępowania zamknięte, zapoznanie z dokumentacją za zamkniętymi drzwiami, i streszczenia są przykładami takich zabezpieczeń.

7.5.3.5 Państwa i organizacje mogą również przyjmować najlepsze praktyki, takie jak zapewnienie, że środowisko, w którym informacje są zbierane, przechowywane, przetwarzane i przesyłane, jest dostatecznie bezpieczne oraz że kontrole dostępu i upoważnienia są wystarczające do ochrony danych bezpieczeństwa i informacji bezpieczeństwa.

7.6. ZASADY STOSOWANIA WYJĄTKÓW

Zasady ochrony mają zastosowanie do danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł, chyba że właściwy organ stwierdzi, że zastosowanie ma jedna z trzech zasad stosowania wyjątków. Wyznaczony podmiot (osoba) odpowiedzialny za ochronę SDCPS powinien być świadomy zabezpieczeń stosowanych do danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł oraz powinien zapewnić, że są one ujawniane i wykorzystywane w zgodzie z przepisami Załącznika 19.

7.6.2 Wyznaczenie właściwego organu

7.6.2.1 Ponieważ zasady stosowania wyjątków będą wykorzystywane w wielu różnych celach, właściwy organ będzie się różnił w zależności od charakteru danych lub informacji oraz rodzaju poszukiwanego zastosowania. W każdym konkretnym przypadku zadaniem właściwego organu będzie podjęcie decyzji, czy ma zastosowanie szczególna zasada stosowania wyjątków. Właściwy organ musi być w stanie równoważyć konkurencyjne interesy, takie jak prawo do wiedzy, przepisy niezwiązane z bezpieczeństwem lotniczym, zasady ujawniania sporów sądowych i inne, w taki sposób, aby społeczeństwo miało zaufanie do jego zdolności decyzyjnych. Właściwe organy mogłyby obejmować organy sądowe, organy regulacyjne lub inne podmioty, którym powierzono obowiązki w zakresie lotnictwa, wyznaczone zgodnie z prawem krajowym i innymi obowiązującymi wymaganiami.

7.6.2.2 Państwa i organizacje będą musiały określić właściwe organy odpowiednie do realizacji zadania polegającego na zastosowaniu zasad stosowania wyjątków dla różnych celów. Tabela 9 poniżej przedstawia przykłady możliwych właściwych organów oraz przykłady sytuacji.

Tabela 9. Przykładowe sytuacje i możliwe właściwe organy

<i>Przykładowa sytuacja</i>	<i>Możliwy właściwy organ</i>
Poszukiwanie możliwości ujawnienia lub wykorzystania danych bezpieczeństwa lub informacji bezpieczeństwa przez członka społeczeństwa zgodnie z przepisami o informacji publicznej ⁵ .	Departament rządowy lub organ administracyjny
Ujawnienie lub wykorzystanie danych lub informacji samo w sobie staje się przedmiotem sporu toczącego się na podstawie tych samych przepisów o informacji publicznej lub poszukiwanie możliwości wykorzystania danych bezpieczeństwa lub informacji bezpieczeństwa w postępowaniach sądowych.	Sąd lub trybunał administracyjny
Podjęcie działań przez organ regulacyjny w celu utrzymania lub poprawy bezpieczeństwa	organ lotnictwa cywilnego (ULC)
Ujawnienie lub wykorzystanie danych bezpieczeństwa lub informacji bezpieczeństwa znajdujących się pod nadzorem organizacji.	Osoba w organizacji odpowiedzialna za bezpieczeństwo lotnicze, taka jak kierownik lub zespół składający się z przedstawicieli kierownictwa, pracowników oraz, w niektórych Państwach, przedstawiciela organu regulacyjnego.

7.6.2.3 W przypadku, gdy organizacja identyfikuje właściwy organ, odpowiedzialne korzystanie z prawa decydowania właściwego organu w sprawie zastosowania zasad stosowania wyjątków i zasad ochrony może również zapewnić wystarczającą samokontrolę w ramach organizacji. Ostateczne określenie właściwego organu dla każdego konkretnego celu pozostaje w gestii każdego państwa i organizacji, w zależności od obowiązujących przepisów i polityk.

7.6.2.4 Stałe wyznaczenie urzędu i jurysdykcji właściwego organu (np. organów sądowych w sprawach związanych z postępowaniem sądowym, władz lotnictwa cywilnego w sprawach związanych z działaniami

⁵ W celu uzyskania dodatkowych informacji dotyczących przepisów o informacji publicznej, patrz pkt 7.7 w niniejszym Rozdziale.

regulacyjnymi) umożliwi szybkie podejmowanie decyzji. Stałe wyznaczenie zapewni również pewność co do pozycji i doświadczenia właściwego organu w zajmowaniu się tego rodzaju sprawami. Ponadto bardzo ważne jest, aby właściwy organ ustanowił zasady i procedury regulujące proces podejmowania decyzji. Te zasady i procedury powinny wynikać z obowiązujących przepisów krajowych. Można to osiągnąć tylko wtedy, gdy wyznaczenie właściwego organu w danym obszarze ma charakter stały.

7.6.3 Zastosowanie zasad stosowania wyjątków

7.6.3.1 Pierwszy przypadek, w którym właściwy organ może zdecydować, że ma zastosowanie wyjątek od ochrony, ma miejsce wtedy gdy występują „fakty i okoliczności wskazujące na to, że zdarzenie mogło być spowodowane działaniem lub zaniechaniem, zgodnie z prawem krajowym, będące zachowaniem stanowiącym rażące zaniedbanie, działanie umyślne lub działalność przestępczą”. Właściwym organem do podjęcia takiej decyzji będzie w większości przypadków organ sądowy, administracyjny lub prokuratorski.

7.6.3.2 Ponieważ ocena treści danych bezpieczeństwa lub informacji bezpieczeństwa często wskazuje, czy dane zachowanie spełnia jeden lub drugi warunek wyjątkowego użycia, nie jest konieczne, aby fakty i okoliczności sprawy jednoznacznie wskazywały, że takie wyjątkowe zachowanie miało miejsce. Konieczne jest jedynie, aby te fakty i okoliczności stanowiły rozsądną podstawę, na której można stwierdzić, że zdarzenie mogło być spowodowane przez takie zachowanie. W przypadku gdy właściwy organ stwierdza, na podstawie faktów i okoliczności sprawy, że zdarzenie mogło być wynikiem rażącego zaniedbania, działania umyślnego lub działalności przestępczej, zgodnie z terminami prawa krajowego, zastosowanie ma zasada stosowania wyjątków, a dane bezpieczeństwa, informacje bezpieczeństwa lub powiązane źródła mogą zostać ujawnione.

7.6.3.3 Różne systemy prawne mogą mieć różne rozumienie zgodnie z prawem krajowym, co należy rozumieć przez te terminy. Ogólnie rzecz biorąc, rażące zaniedbanie odnosi się do działania lub zaniechania podjętego z poważnym lekceważeniem lub obojętnością na oczywiste ryzyko, niezależnie od tego, czy ryzyko zostało w pełni ocenione przez osobę dopuszczającą się tych czynów. Jest ono czasami określane jako lekkomyślne zachowanie. Działanie umyślne to bezprawne działanie lub zaniechanie, co do którego osoba dopuszczająca się takich czynów wie, że jest bezprawne lub jest świadomie obojętna na pytanie, czy jest ono bezprawne, czy nie. Wiedza i zamiary w takich przypadkach mogą czasami uwzględniać konsekwencje zachowania, ale nie jego formalne zobrazowanie jako czynu niezgodnego z prawem. W każdym przypadku, testy dowodowe i środki mające zastosowanie przy ustalaniu charakteru danego zachowania powinny być zgodne z prawem odpowiedniej jurysdykcji. Ponadto, ponieważ zasada stosowania wyjątków rozróżnia pomiędzy zachowaniem stanowiącym „rażące zaniedbanie” lub „działanie umyślne”, z jednej strony, a „działalność przestępczą” z drugiej, jasne jest, że zachowanie, które może stanowić „rażące zaniedbanie” lub „działanie umyślne” (jednakże takie zachowanie może być opisane zgodnie z obowiązującym prawem krajowym) ma być oceniane na podstawie norm cywilnych, a nie karnych.

7.6.3.4 Drugi przypadek, w którym właściwy organ może zdecydować, że wyjątek od zasady ochrony ma zastosowanie, ma miejsce, jeżeli po przeanalizowaniu danych bezpieczeństwa lub informacji bezpieczeństwa, właściwy organ stwierdza, że ujawnienie takich danych lub informacji jest „niezbędne dla właściwego funkcjonowania wymiaru sprawiedliwości” oraz „korzyści płynące z ujawnienia przeważają nad niekorzystnym wpływem, jaki to ujawnienie może mieć na zbieranie i dostępność danych i informacji w przyszłości w skali krajowej i międzynarodowej”.

7.6.3.5 Jest to dwuetapowy proces oceny, w którym właściwy organ musi najpierw rozważyć, czy dane lub informacje są „niezbędne do prawidłowego funkcjonowania wymiaru sprawiedliwości”, co może nie mieć miejsca, jeżeli dostępne są alternatywne źródła tych samych informacji; i po drugie, jeżeli stwierdzi, że ujawnienie jest konieczne dla prawidłowego funkcjonowania wymiaru sprawiedliwości, czy, w sumie, wartość takich danych lub informacji przeważa nad szkodą, jaką może mieć ich ujawnienie, w zbieraniu i dostępności danych i informacji w przyszłości w celu utrzymania lub poprawy bezpieczeństwa.

7.6.3.6 Jeżeli dane bezpieczeństwa lub informacje bezpieczeństwa są proponowane do wykorzystania w działaniu lub postępowaniu (cywilnym, administracyjnym, karnym lub dyscyplinarnym), potencjalny negatywny wpływ wynikający z takiego użycia może dotyczyć źródła danych lub informacji. Nawet jeżeli można wprowadzić zabezpieczenia mające na celu zapobieganie ujawnieniu danych bezpieczeństwa lub informacji bezpieczeństwa poza zakres działania lub postępowania, jakkolwiek negatywny wpływ wykorzystania takich danych lub informacji podczas postępowania może nadal zniechęcać do zgłaszania w przyszłości lub ujawniania danych bezpieczeństwa i informacji bezpieczeństwa w celu utrzymania lub poprawy bezpieczeństwa. Jeżeli proponowane wykorzystanie danych bezpieczeństwa lub informacji bezpieczeństwa wiąże się z rozpowszechnianiem lub publikacją takich danych lub informacji poza zakres postępowania, właściwy organ powinien również rozważyć potencjalny szkodliwy wpływ na szerszą społeczność (krajową i międzynarodową).

7.6.3.7 Na poziomie indywidualnym, upublicznienie informacji może mieć szkodliwy wpływ na osobę zaangażowaną, np. zakłopotanie i/lub potencjalna utrata środków do życia. Na szerszym poziomie, publikacja lub rozpowszechnianie danych bezpieczeństwa lub informacji bezpieczeństwa w konkretnym przypadku może stanowić ogólny czynnik zniechęcający dla osób znajdujących się w podobnej sytuacji, ale nie uczestniczących w danym działaniu lub postępowaniu, do zgłaszania lub przyczyniania się do gromadzenia takich danych i informacji.

7.6.3.8 Ustalając pierwsze dwie zasady stosowania wyjątków, właściwy organ musi być przekonany, że:

- a) w pierwszym przypadku: treść danych bezpieczeństwa lub informacji bezpieczeństwa, które mają być ujawnione lub wykorzystane, wymaga określenia czy działanie lub zaniechanie stanowi rażące zaniechanie, działanie umyślne lub działalność przestępczą; lub
- b) w drugim przypadku: takie dane, informacje lub powiązane źródło są niezbędne dla właściwego funkcjonowania wymiaru sprawiedliwości.

7.6.3.9 Właściwy organ określi, czy dane bezpieczeństwa, informacje bezpieczeństwa lub tożsamość źródła takich danych lub informacji są niezbędne dla danej sprawy. Jeżeli właściwy organ może podjąć decyzję bez odwoływania się do chronionych danych, informacji lub źródła, wówczas należy zwrócić większą uwagę na zachowanie ochrony danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł. Nie ma konieczności powodowania szkód w zbieraniu i dostępności danych bezpieczeństwa, informacji bezpieczeństwa i związanych z nimi źródeł, jeżeli właściwy organ może podjąć decyzję bez konieczności ujawniania (lub wykorzystania) takich danych i informacji. Pomoże to zapewnić ciągłą dostępność danych bezpieczeństwa i informacji bezpieczeństwa w celu utrzymania lub poprawy bezpieczeństwa lotniczego.

7.6.3.10 Niepożądane konsekwencje, jakie mogą wynikać z ujawnienia lub wykorzystywania danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł, to niechęć personelu operacyjnego do dobrowolnej współpracy z inspektorami. Jeżeli takie dane, informacje lub szczegóły dotyczące ich źródeł nie są konieczne do udowodnienia istotnego faktu w postępowaniu, to przyszłe zbieranie i dostępność danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł nie powinny być zagrożone poprzez zbędne ujawnianie na mocy jednej z zasad stosowania wyjątków. Ponadto, jeżeli wymagane informacje można w praktyce uzyskać z alternatywnych źródeł, właściwy organ może podjąć decyzję o uniemożliwieniu dostępu do danych bezpieczeństwa lub informacji bezpieczeństwa, dopóki nie zostaną wyczerpane wszystkie rozsądne alternatywne sposoby uzyskania informacji.

7.6.3.11 Podobnie, jeżeli właściwy organ danego Państwa, które nie posiada przepisów o informacji publicznej, zostanie poproszony o podjęcie decyzji, czy dane bezpieczeństwa lub informacje bezpieczeństwa powinny być ujawnione opinii publicznej (na przykład w odpowiedzi na prośbę mediów), właściwy organ najprawdopodobniej chciałby wiedzieć, jak ważne jest, aby opinia publiczna знаła treść takich danych lub informacji. W takiej sytuacji właściwy organ może zadać pytanie typu „Czy bez znajomości treści danych lub informacji, opinia publiczna posiada odpowiednią wiedzę na temat zdarzenia, lub, czy zdarzenie będzie miało konsekwencje w zakresie bezpieczeństwa dla podróżujących?”. Uzasadnienie poglądu, że wiedza społeczeństwa byłaby zagrożona bez dostępu do danych bezpieczeństwa lub informacji bezpieczeństwa, mogłaby przydać wagi

argumentowi za ich ujawnieniem. Jednak te dane lub informacje nie musiałyby być ujawniane tylko dlatego, że takie podstawy zostały ustalone. Jeżeli ujawnienie poważnie zagroziłoby ciągłej dostępności danych bezpieczeństwa i informacji bezpieczeństwa zniechęcając do zgłaszania zdarzeń dotyczących bezpieczeństwa w przyszłości, szala nie musi przechylać się na korzyść ujawnienia.

7.6.3.12 Trzeci wyjątek obejmuje przypadki, w których „po dokonaniu przeglądu danych bezpieczeństwa lub informacji bezpieczeństwa” właściwy organ „stwierdza, że ich ujawnienie jest niezbędne do utrzymania lub poprawy bezpieczeństwa oraz że korzyści płynące z ujawnienia przeważają nad niekorzystnym wpływem, jaki to ujawnienie może mieć na zbieranie i dostępność danych i informacji w przyszłości w skali krajowej i międzynarodowej”. Ten wyjątek dotyczy ujawnienia danych bezpieczeństwa lub informacji bezpieczeństwa niezbędnych do utrzymania lub poprawy bezpieczeństwa. Nie ma zastosowania do wykorzystywania danych bezpieczeństwa lub informacji bezpieczeństwa w związku z działaniami zapobiegawczymi, naprawczymi lub zaradczymi podejmowanymi przez organ regulacyjny, które są niezbędne do utrzymania lub poprawy bezpieczeństwa lotniczego.

7.6.3.13 Okoliczności przewidziane w Załączniku 19 obejmują uwzględnienie przez właściwy organ korzyści płynących z ujawnienia danych bezpieczeństwa lub informacji bezpieczeństwa dla bardziej ogólnych celów związanych z utrzymaniem lub poprawą bezpieczeństwa, w tym, na przykład, celów szkoleniowych i edukacyjnych lub publikacją informacji i porad dotyczących bezpieczeństwa na rzecz szerszej społeczności. Analiza tych sytuacji obejmuje ten sam rodzaj dwustopniowego procesu opisanego w pkt 7.6.3.5 powyżej: po pierwsze, wymaganie, aby właściwy organ podjął decyzję, że „ujawnienie jest konieczne do utrzymania lub poprawy bezpieczeństwa”, i po drugie, wymaganie, aby właściwy organ określił, że korzyści z ujawnienia danych bezpieczeństwa lub informacji bezpieczeństwa przeważają nad potencjalnym niekorzystnym wpływem, jaki takie ujawnienie będzie miało na zbieranie i dostępność takich danych i informacji w przyszłości.

7.6.3.14 Rozważając drugi etap tej analizy, Załącznik 19 zachęca właściwe organy do uwzględnienia „zgody źródła danych bezpieczeństwa i informacji bezpieczeństwa”. Znaczenie tego uznania podkreśla krytyczne rozróżnienie omówione w pkt 7.4.2 powyżej, rozróżniając pomiędzy ujawnianiem danych bezpieczeństwa i informacji bezpieczeństwa do celów ogólnie związanych z utrzymaniem lub poprawą bezpieczeństwa (w którym to przypadku zastosowanie ma zasada stosowania wyjątków), oraz wykorzystaniem danych bezpieczeństwa i informacji bezpieczeństwa do szczególnych celów zapobiegawczych, naprawczych i zaradczych w celu utrzymania lub poprawy bezpieczeństwa (w takim przypadku nie będzie konieczne spełnienie wymogów jakiegokolwiek zasady stosowania wyjątków, ponieważ to użycie jest już dozwolone w ramach zasad ochrony).

7.6.3.15 Zgodnie z duchem zasad ochrony, rozważając wykorzystanie danych bezpieczeństwa lub informacji bezpieczeństwa w celu wsparcia działań zapobiegawczych, naprawczych lub zaradczych podjętych w celu utrzymania lub poprawy bezpieczeństwa, właściwy organ może ustalić czy odpowiednie alternatywne źródło takich danych lub informacji może być praktycznie dostępne. Jeżeli tak, można uniknąć nawet tego nie wyjątkowego wykorzystania chronionych danych bezpieczeństwa lub informacji bezpieczeństwa.

7.6.3.16 Jednakże takie rozważenie wykonalności nie wymaga ani nie zachęca do formalnego zastosowania zasady stosowania wyjątków, o której mowa w Załączniku 19. Dzieje się tak, ponieważ zasada stosowania wyjątków ma zastosowanie, gdy interes utrzymania lub poprawy bezpieczeństwa jest przeciwstawiany innemu konkurencyjnemu interesowi publicznemu (np. właściwe funkcjonowanie wymiaru sprawiedliwości, zapewnienie publicznego dostępu do danych lub informacji, lub ułatwienie procesów szkoleniowych lub edukacyjnych poprzez umożliwienie włączenia chronionych danych lub informacji). Działania zapobiegawcze, naprawcze lub zaradcze podjęte w celu utrzymania lub poprawy bezpieczeństwa wchodzą w zakres zasad ochrony i nie ma przeciwdziałających interesów niezwiązanych z bezpieczeństwem, wobec których takie zastosowanie wymaga zrównoważenia.

7.6.4 Dodatkowe uwarunkowania związane z zastosowaniem zasady stosowania wyjątków

7.6.4.1 Przy podejmowaniu decyzji, czy zasada stosowania wyjątków ma zastosowanie w danej sprawie, właściwy organ powinien zawsze uwzględnić zgodę źródła danych bezpieczeństwa lub informacji bezpieczeństwa. Jeżeli dana osoba otrzymała gwarancje poufności w odniesieniu do danych bezpieczeństwa lub informacji bezpieczeństwa, których jest źródłem, wówczas użycie, udostępnienie lub ujawnienie takich danych lub informacji w sposób sprzeczny z tymi gwarancjami może mieć niekorzystny wpływ na zgłaszanie danych bezpieczeństwa i informacji bezpieczeństwa przez tę osobę w przyszłości. Ponadto, jeżeli dane bezpieczeństwa lub informacje bezpieczeństwa miałyby zostać ujawnione lub wykorzystane pomimo gwarancji poufności dla źródła, może to wpływać w podobny niekorzystny sposób na każdą osobę, która może się o tym dowiedzieć.

7.6.4.2 Aby uniknąć niepożądanych sytuacji, o których mowa w pkt 7.6.4.1, należy upewnić się, że osoby fizyczne i organizacje z wyprzedzeniem rozumieją, w jaki sposób, kiedy, gdzie i w jakim celu mogą być wykorzystywane dane i informacje, które są przez nich przekazywane, w sytuacji kiedy mają zastosowanie zasady stosowania wyjątków. Takie zrozumienie jest niezbędne do ustanowienia i utrzymania przewidywalnego środowiska zgłaszania opartego na zaufaniu.

7.6.4.3 Ogólne wytyczne dotyczące zastosowania zasad stosowania wyjątków przez właściwy organ zgodne z przepisami Załącznika 19 przedstawione zostały na Rysunku 7-2.⁶

7.7. UPUBLICZNIANIE

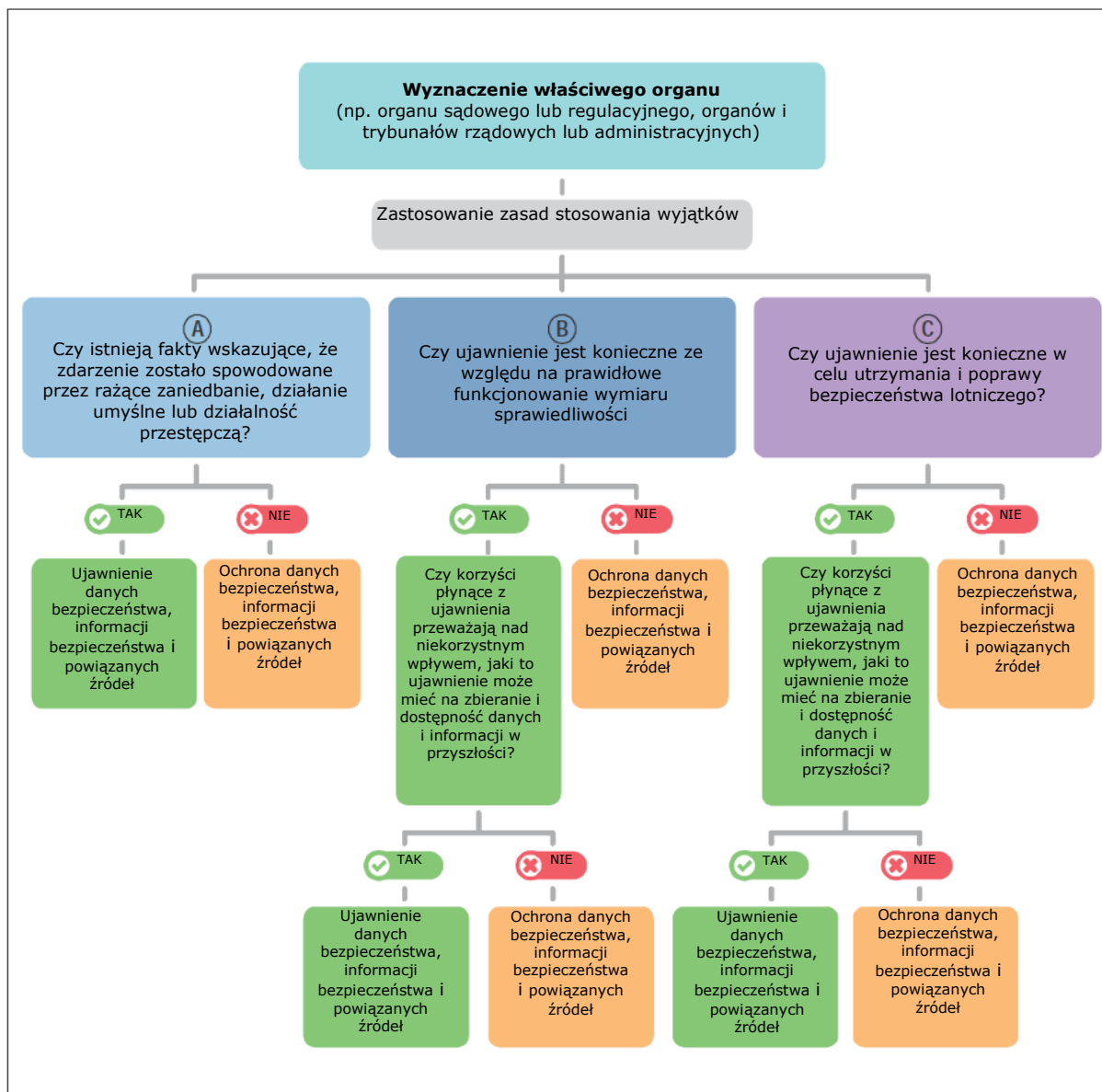
7.7.1 Nadrzędny interes w zakresie danych bezpieczeństwa lub informacji bezpieczeństwa posiada społeczeństwo. Opinia publiczna jest zainteresowana otwartością, przejrzystością i odpowiedzialnością, tak aby posiadać ogólną świadomość bezpieczeństwa systemu i mieć pewność, że wszystko, co jest konieczne dla zapewnienia bezpieczeństwa, jest realizowane. Określone osoby lub grupy interesów mogą również być zainteresowane danymi bezpieczeństwa lub informacjami bezpieczeństwa z powodów innych niż te bezpośrednio związane z bezpieczeństwem. Ujawnienie danych lub informacji może mieć miejsce dobrowolnie w wyniku prośby o informacje skierowanej do rządu lub w ramach postępowania sądowego. Zasadność upublicznienia jakichkolwiek danych bezpieczeństwa lub informacji bezpieczeństwa zależy od charakteru danych bezpieczeństwa i informacji bezpieczeństwa. Jak zostało to wcześniej omówione, decyzja taka leży w zakresie właściwego organu.

7.7.2 Jeżeli dane bezpieczeństwa lub informacje bezpieczeństwa są upubliczniane, zazwyczaj nie ma możliwości ograniczenia zakresu, w jakim informacje zostaną wykorzystane. Oczywiście należy zachęcać do otwartości i przejrzystości, ale jednocześnie należy wziąć pod uwagę prawa i uzasadnione oczekiwania osób zaangażowanych w zgłaszanie i analizowanie danych bezpieczeństwa i informacji bezpieczeństwa oraz potrzebę ochrony ich interesów lub reputacji. Jednak nie zawsze może to mieć zastosowanie do Państw, w których obowiązują przepisy o informacji publicznej.

7.7.3 Wiele Państw posiada ustawodawstwo, które w efekcie wymaga ujawnienia wszystkich informacji będących w posiadaniu instytucji państwowych. Takie prawo jest czasami określane jako prawo do informacji publicznej. Zgodnie z tymi przepisami, chyba że istnieje zwolnienie dotyczące określonego rodzaju informacji, informacje muszą być ujawnione przez rząd na wniosek. Niektórymi przykładami zwolnień mogą być informacje niejawne, wrażliwe informacje handlowe lub informacje takie jak dokumentacja medyczna, które chronione są prawem prywatności. Dane bezpieczeństwa lub informacje bezpieczeństwa nie są zazwyczaj zwolnione. Zgodnie z Załącznikiem 19 Państwa mogą zdecydować o określeniu zwolnień lub zasad mających na celu ochronę przed

⁶ Ważne jest, aby pamiętać, że Państwom nie należy zakazywać korzystania z danych dotyczących bezpieczeństwa lub informacji dotyczących bezpieczeństwa w celu podjęcia jakichkolwiek działań zapobiegawczych, naprawczych lub zaradczych, które są niezbędne do utrzymania lub poprawy bezpieczeństwa lotniczego.

upublicznieniem w przepisach o informacji publicznej lub w jakimkolwiek innym rodzaju przepisów, w tym przepisów dotyczących lotnictwa.



Rysunek 7-2. Wytyczne w zakresie zastosowania zasad stosowania wyjątków

7.7.4 Prawo do informacji publicznej ma zwykle zastosowanie do informacji będących w posiadaniu administracji rządowej. Ponieważ większość danych bezpieczeństwa i informacji bezpieczeństwa wymagających ochrony przed ujawnieniem jest uzyskiwana od personelu operacyjnego lub podmiotu lotniczego, praktyczne podejście polegałoby na pozostawieniu takich danych i informacji w organizacji zamiast deponowania ich w organach rządowych. W ten sposób, kwestia upubliczniania nie pojawia się, chyba że zainicjowane zostanie działanie rządu w formie postępowania administracyjnego. W przypadku gdy kwestia upubliczniania ma miejsce w postępowaniu administracyjnym lub sądowym, właściwy organ powinien zastosować podstawowe zasady ochrony omówione wcześniej. Takie podejście może nie zadziałać, jeżeli podmioty lotnicze są zobowiązane do zgłaszania danych bezpieczeństwa i informacji bezpieczeństwa organowi rządowemu lub jeżeli podmiot lotniczy jest organem lub agencją rządową lub częścią organu lub agencji rządowej.

7.7.5 Brak właściwej oceny konkurencyjnych roszczeń dotyczących dostępu do danych bezpieczeństwa lub informacji bezpieczeństwa może wpłynąć na bieżące i przyszłe działania na dwa sposoby. Upublicznienie pewnych

danych lub informacji może być postrzegane jako naruszenie prywatności osób lub oczekiwań dotyczących poufności organizacji związanych z danymi bezpieczeństwa lub informacjami bezpieczeństwa. Wykorzystanie pewnych danych lub informacji jako argumentu popierającego sankcje przeciwko zaangażowanym osobom lub organizacjom może być postrzegane jako naruszenie podstawowych zasad sprawiedliwości. Dostępność danych bezpieczeństwa i informacji bezpieczeństwa w przyszłości może wynikać z przewidywalnych ludzkich zachowań polegających na wstrzymywaniu informacji w związku z przewidywanym zagrożeniem wynikającym z ich ujawnienia lub obciążającego wykorzystania. Może to mieć oczywisty wpływ zarówno na funkcje zbierania danych jak i analizy danych w procesie zarządzania bezpieczeństwem.

7.7.6 Jeżeli właściwy organ stwierdzi, że dane bezpieczeństwa lub informacje bezpieczeństwa mogą zostać upublicznione, oczekuje się, że Państwo zapewni, że każde publiczne ujawnienie zostanie dokonane zgodnie z obowiązującymi przepisami dotyczącymi prywatności lub w formie pozbawionej elementów pozwalających na identyfikację, podsumowującej lub zagregowanej. Dalsze informacje na temat wiarygodnych zabezpieczeń znajdują się w pkt 7.5.3.

7.8. OCHRONA ZAREJESTROWANYCH DANYCH

7.8.1 Ochrona nagrań w miejscu pracy

7.8.1.1 Nagrania w miejscu pracy powinny być częścią każdej polityki lub regulacji w zakresie ochrony. Wykorzystanie tych nagrań jako część zarządzania bezpieczeństwem, jeżeli pozwalają na to przepisy lub polityka, powinno być w pełni zgodne z zasadami ochrony i zasadami stosowania wyjątków. Zaufanie ze strony osób zgłaszających ma fundamentalne znaczenie dla skutecznego zarządzania bezpieczeństwem. Zaufanie to nie powinno być zagrożone.

7.8.1.2 Przepisy zawarte w Załączniku 19 mają zastosowanie do funkcji zarządzania bezpieczeństwem związanych z bezpieczną eksploatacją statków powietrznych lub bezpośrednio je wspierających. Nagrania w miejscu pracy mogą podlegać krajowym przepisom dotyczącym prywatności, które nie są zdefiniowane w Załączniku 19.

7.8.1.3 Nagrania w miejscu pracy mogą obejmować CVR, AIR, inne zapisy rejestratorów lotu lub nagrania łączności w tle i środowiska dźwiękowego na stanowiskach pracy kontrolerów ruchu lotniczego.

7.9. UDOSTĘPNIANIE I WYMIANA INFORMACJI BEZPIECZEŃSTWA

7.9.1 Ochrona informacji udostępnianych pomiędzy Państwami

7.9.1.1 Biorąc pod uwagę, że jednym z głównych celów udostępniania i wymiany informacji bezpieczeństwa jest zapewnienie spójnej, opartej na faktach i przejrzystej reakcji na obawy dotyczące bezpieczeństwa na szczeblu krajowym i globalnym, w procesie udostępniania i wymiany informacji bezpieczeństwa, Państwa działają zgodnie z następującymi zasadami:

- a) zachowana jest zgodność z Konwencją o międzynarodowym lotnictwie cywilnym (Konwencja Chicagowska), jej załącznikami oraz innymi wielostronnymi i dwustronnymi zobowiązaniami Państw;
- b) udostępnianie i wymiana informacji bezpieczeństwa nie prowadzi do naruszenia przez odpowiednie organy Państw prawa krajowego odnoszącego się do ochrony informacji bezpieczeństwa, w tym między innymi krajowych przepisów i regulacji dotyczących tajemnicy państwowej, ochrony danych osobowych, tajemnicy handlowej jak również naruszenia praw osób fizycznych i prawnych;

- c) informacje bezpieczeństwa udostępniane i wymieniane przez Państwo nie powinny być wykorzystywane w sposób niekorzystnie wpływający na takie Państwo, jego linie lotnicze, urzędników państwowych i jego obywateli, a także dla innych nieodpowiednich celów, w tym w celu uzyskania korzyści ekonomicznych;
- d) jedynym celem ochrony informacji bezpieczeństwa przed niewłaściwym użyciem jest zapewnienie ich ciągłej dostępności, tak aby można było podjąć właściwe i terminowe działania zapobiegawcze oraz poprawić bezpieczeństwo lotnicze; oraz
- e) zasady udostępniania i wymiany informacji dotyczących bezpieczeństwa powinny być zgodne z zasadami ochrony określonymi w Załączniku 19.

7.9.1.2 Ramy prawne dotyczące udostępniania i wymiany informacji mogą opierać się na porozumieniach dwustronnych pomiędzy Państwami dołączonych do, na przykład, umowy o transporcie lotniczym (usługach lotniczych). Aby ułatwić udostępnianie i wymianę informacji, Państwa mogą również uzgodnić, że takie umowy dwustronne mają zastosowanie tymczasowe, w stosownych przypadkach, w oczekiwaniu na ich ratyfikację i wejście w życie.

7.9.1.3 Państwa powinny promować i ułatwiać tworzenie sieci udostępniania i wymiany informacji bezpieczeństwa pomiędzy użytkownikami swojego systemu lotniczego. Udostępnianie i wymiana informacji bezpieczeństwa ma zasadnicze znaczenie dla zapewnienia spójnej, opartej na faktach i przejrzystej reakcji na obawy dotyczące bezpieczeństwa na szczeblu krajowym i globalnym.

ROZDZIAŁ 8

ODPOWIEDZIALNOŚĆ PAŃSTWA ZA ZARZĄDZANIE BEZPIECZEŃSTWEM

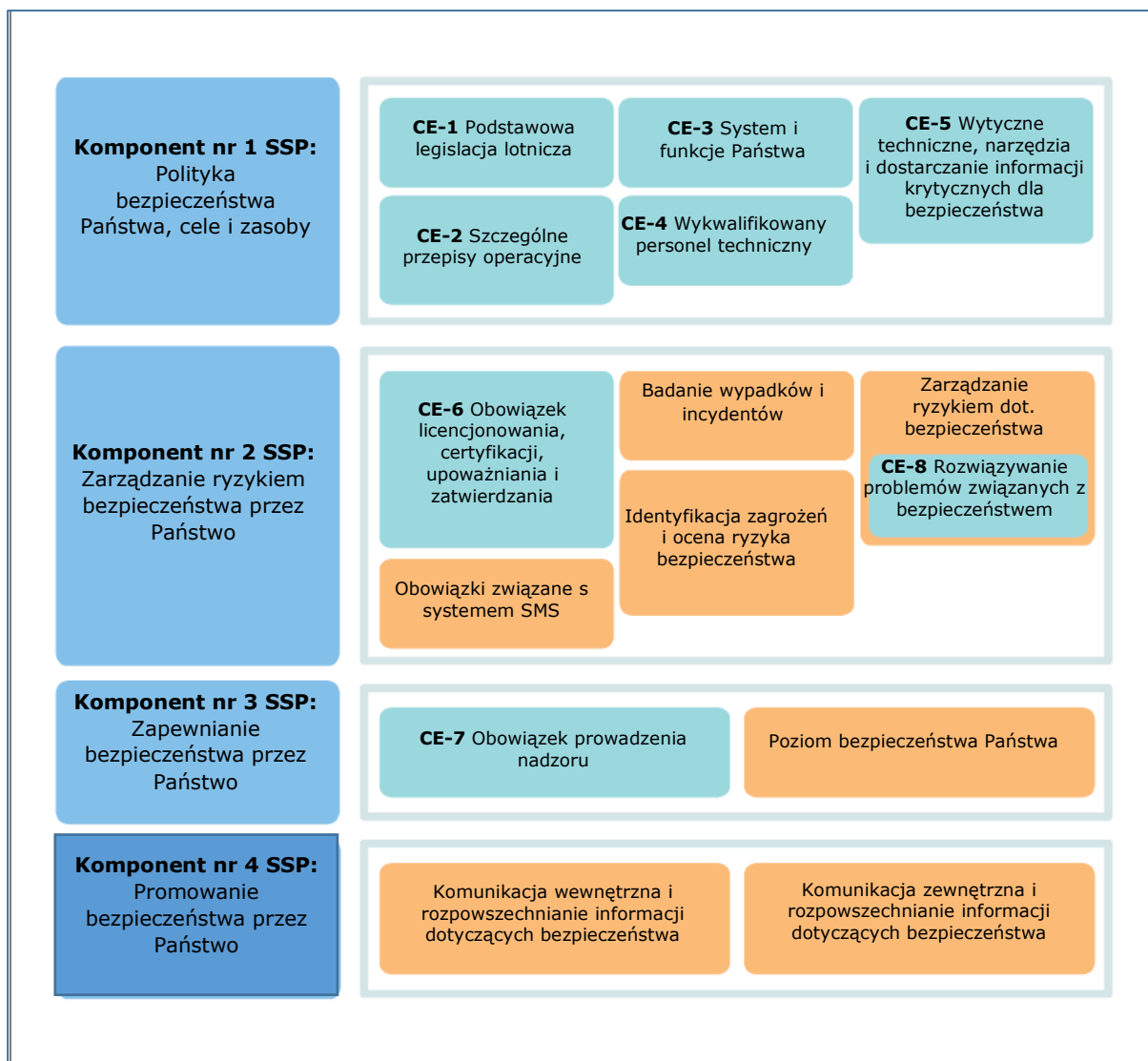
8.1. WSTĘP

8.1.1 Rozdział 3 Załącznika 19 zawiera normy i zalecane metody postępowania związane z odpowiedzialnością Państwa za zarządzanie bezpieczeństwem. Dotyczy to ustanowienia i utrzymania krajowego programu bezpieczeństwa (SSP), którego celem jest zarządzanie bezpieczeństwem w sposób zintegrowany.

8.1.2 Zgodnie z przepisami zawartymi w pierwszym wydaniu Załącznika 19, Państwa miały ustanowić i wdrożyć dwa zestawy przepisów, było to osiem elementów krytycznych (CE) krajowego systemu nadzoru nad bezpieczeństwem (SSO) oraz cztery komponenty krajowego programu bezpieczeństwa. Aspekt dotyczący nadzoru nad bezpieczeństwem odzwierciedlał tradycyjną rolę Państwa, polegającą na zapewnieniu skutecznego wdrożenia przez branżę lotniczą nakazowych norm i zalecanych metod postępowania (SARP), podczas gdy SSP stanowił włączenie zasad zarządzania bezpieczeństwem. Szczegółowe informacje na temat ośmiu elementów krytycznych znajdowały się w Dodatku 1 do Załącznika i posiadały status SARP, a szczegółowe elementy struktury wdrażania i utrzymania SSP zostały przedstawione w Załączniku A w formie wytycznych.

8.1.3 Krajowy system nadzoru nad bezpieczeństwem i SSP były ściśle powiązane pod względem celów bezpieczeństwa, które każdy z nich stara się osiągnąć. Obydwa dotyczą funkcji i obowiązków Państwa, z czego system nadzoru przede wszystkim w odniesieniu do nadzoru nad bezpieczeństwem, natomiast SSP w odniesieniu do zarządzania bezpieczeństwem i poziomu bezpieczeństwa. Istnieją pewne aspekty zarządzania bezpieczeństwem w ośmiu elementach krytycznych, które odzwierciedlają przejście do proaktywnego podejścia do zarządzania bezpieczeństwem. Na przykład, obowiązki prowadzenia nadzoru (CE-7) można uznać za element zapewniania bezpieczeństwa, a podstawowa legislacja lotnicza (CE-1) oraz szczególne przepisy operacyjne (CE-2) zostały również odzwierciedlone w pierwotnej strukturze SSP jako ważne elementy kontroli ryzyka bezpieczeństwa.

8.1.4 Obowiązki te zostały uwzględnione w drugim wydaniu Załącznika 19 i są zbiorczo określane jako odpowiedzialność Państwa za zarządzanie bezpieczeństwem. SARP dotyczące odpowiedzialności Państwa za zarządzanie bezpieczeństwem, które obejmują zarówno nadzór nad bezpieczeństwem, jak i zarządzanie bezpieczeństwem, są współzależne i stanowią zintegrowane podejście do skutecznego zarządzania bezpieczeństwem. Chociaż termin SSP jest nadal używany w drugim wydaniu Załącznika 19, jego znaczenie zmieniło się i obejmuje zintegrowany zestaw norm i zalecanych metod postępowania zawartych w Rozdziale 3. Jako taki, SSP nie jest już opisywany jako struktura, ale raczej jako program służący spełnieniu odpowiedzialności Państwa za zarządzanie bezpieczeństwem, który obejmuje nadzór nad bezpieczeństwem. Tak więc SSP jest częścią szerokiej koncepcji zarządzania bezpieczeństwem przez Państwo. Ewolucja ta została przedstawiona na Rysunku 8-1.



Rysunek 8-1. Zintegrowany krajowy program bezpieczeństwa

8.2. KRAJOWY PROGRAM BEZPIECZEŃSTWA (SSP)

8.2.1 Elementy krytyczne krajowego systemu nadzoru nad bezpieczeństwem

Elementy krytyczne (CE) krajowego systemu nadzoru nad bezpieczeństwem (SSO) stanowią podstawę krajowego programu bezpieczeństwa (SSP). Drugie wydanie Załącznika 19 podkreśla znaczenie systemu nadzoru nad bezpieczeństwem poprzez utrzymanie przepisów dotyczących ośmiu elementów krytycznych na poziomie normy. Większość wymagań ze struktury SSP została podniesiona do kategorii zalecanych norm postępowania, a kilka zostało podniesionych do normy. Szczegółowe informacje dotyczące elementów krytycznych krajowego systemu nadzoru nad bezpieczeństwem znajdują się w *Podręczniku nadzoru nad bezpieczeństwem, Część A – Ustanowienie i zarządzanie krajowym systemem nadzoru nad bezpieczeństwem* (Doc 9734).

8.2.2 Przegląd krajowego programu bezpieczeństwa

8.2.2.1 SSP to zintegrowany zestaw przepisów i działań mających na celu poprawę bezpieczeństwa. W celu ustanowienia i utrzymania SSP, normy i zalecane metody postępowania ICAO posiadają strukturę, w skład której wchodzi cztery poniższe komponenty:

- a) polityka bezpieczeństwa Państwa, cele i zasoby;
- b) zarządzanie ryzykiem bezpieczeństwa przez Państwo;
- c) zapewnienie bezpieczeństwa przez Państwo; oraz
- d) promowanie bezpieczeństwa przez Państwo.

8.2.2.2 Wdrożenie SSP wymaga koordynacji pomiędzy wieloma organami odpowiedzialnymi za funkcje lotnicze Państwa. Wdrożenie SSP nie zmienia ról, jakie odgrywają organizacje lotnicze Państwa ani wzajemnego oddziaływania pomiędzy nimi. Zamiast tego SSP ma na celu wykorzystanie zbiorowych funkcji i możliwości związanych

z bezpieczeństwem w celu jego dalszego wzmocnienia w ramach Państwa. Rozpoczynając wdrażanie SSP, większość Państw stwierdza, że posiada procesy i działania, które dotyczą wielu aspektów SSP. Wdrożenie SSP ma na celu usprawnienie tych procesów poprzez dodatkowe elementy oparte na wydajności i ryzyku bezpieczeństwa oraz ułatwienie skutecznego wdrożenia SMS przez branżę lotniczą danego Państwa.

8.2.2.3 SSP ma na celu:

- a) zapewnienie, że Państwo posiada skuteczne ramy prawne wraz z wspierającymi przepisami operacyjnymi;
- b) zapewnienie koordynacji pomiędzy zarządzaniem ryzykiem bezpieczeństwa (SRM) a zapewnieniem bezpieczeństwa, oraz synergii pomiędzy odpowiednimi organami ds. lotnictwa w danym Państwie;
- c) wsparcie skutecznego wdrożenia i odpowiednią interakcję pomiędzy systemami zarządzania bezpieczeństwem podmiotów lotniczych;
- d) ułatwienie monitorowania i pomiaru poziomu bezpieczeństwa branży lotniczej Państwa; oraz
- e) utrzymywanie i/lub ciągłą poprawę ogólnego poziomu bezpieczeństwa Państwa.

8.2.3 Przekazywanie funkcji i działań związanych z zarządzaniem bezpieczeństwem

8.2.3.1 Niektóre działania związane z zarządzaniem bezpieczeństwem wymagają nowych kompetencji, takich jak prowadzenie ocen ryzyka bezpieczeństwa, wykonywanie analiz danych bezpieczeństwa lub ocena stosowności wskaźników SPI.

8.2.3.2 Państwo może zdecydować o przekazaniu niektórych określonych funkcji lub zadań w ramach SSP innemu Państwu, regionalnej organizacji nadzoru nad bezpieczeństwem (RSOO) lub innej właściwej organizacji, takiej jak stowarzyszenie handlowe, organizacja reprezentująca przemysł lub podmiot prywatny. Chociaż Państwo może delegować określone funkcje, nadal będzie potrzebować wystarczającej liczby personelu, aby współpracować z delegowanym podmiotem i przetwarzać informacje przekazane przez jednostkę delegowaną.

8.2.3.3 Państwa powinny również rozważyć ustanowienie odpowiednich procesów technicznych i administracyjnych w celu zapewnienia, że realizacja przekazanych funkcji przebiega we właściwy sposób.

8.2.3.4 Niezależnie od ustaleń, Państwo zachowuje odpowiedzialność za zapewnienie, że wszelkie delegowane zadania są wykonywane zgodnie z wymaganiami krajowymi i normami SARP.

8.2.3.5 Delegowanie zadań może pozwolić Państwu o stosunkowo niskim poziomie działalności lotniczej na zbiorcze gromadzenie danych bezpieczeństwa w celu określenia trendów i koordynacji strategii łagodzenia.

8.2.3.6 Jeżeli Państwo decyduje się na przyjęcie pomocy na rozwój procesów nadzoru, powinien on obejmować opracowanie profili ryzyka bezpieczeństwa organizacji dla podmiotów lotniczych, planowanie i ustalanie priorytetów inspekcji, audytów i działań monitorujących zatwierdzonej organizacji/podmiotów lotniczych.

8.2.3.7 Jeżeli Państwo zdecyduje się na delegowanie działań w zakresie nadzoru, Państwo powinno zapewnić, że posiada dostęp do rejestrów dotyczących nadzoru wraz z udokumentowanymi wynikami. Państwo powinno również okresowo monitorować i prowadzić przegląd poziomu bezpieczeństwa każdego podmiotu lotniczego, oraz upewnić się, że jednoznacznie określono, kto będzie monitorował i egzekwował (w razie potrzeby) rozwiązywanie wszelkich problemów związanych z bezpieczeństwem.

8.2.3.8 Delegowanie zadań stanowi środek dla Państw o ograniczonych zasobach zapewniający dostęp do odpowiedniej wiedzy specjalistycznej. Wytyczne dotyczące ustanowienia RSOO znajdują się w *Podręczniku nadzoru nad bezpieczeństwem, Część B - Ustanowienie i zarządzanie regionalną organizacją nadzoru nad bezpieczeństwem* (Doc 9734).

8.3. KOMPONENT NR 1: POLITYKA BEZPIECZEŃSTWA PAŃSTWA, CELE I ZASOBY

8.3.1 Pierwszy komponent SSP określa, w jaki sposób Państwo będzie zarządzać bezpieczeństwem w całym swoim systemie lotniczym. Określa wymagania, obowiązki, funkcje i działania różnych władz lotniczych Państwa w zakresie SSP, a także ogólnych celów bezpieczeństwa, które należy osiągnąć. Polityka i cele bezpieczeństwa Państwa powinny być udokumentowane w celu zapewnienia jasnych oczekiwań i utrzymania wysiłków na rzecz zarządzania bezpieczeństwem przez władze lotnicze Państwa, i władze lotnicze innych Państw, skoncentrowane na utrzymaniu i poprawie bezpieczeństwa. Umożliwia to Państwu zapewnienie jasnych wytycznych dotyczących bezpieczeństwa w celu wsparcia systemu transportu lotniczego, który bezustannie rośnie i staje się coraz bardziej złożony.

8.3.2 Ramy prawne Państwa określają sposób zarządzania bezpieczeństwem lotniczym. Podmioty lotnicze są prawnie odpowiedzialne za bezpieczeństwo swoich produktów i usług. Muszą one działać zgodnie z przepisami w zakresie bezpieczeństwa ustanowionymi przez Państwo. Państwo powinno zagwarantować, że władze lotnicze zaangażowane we wdrażanie i utrzymanie SSP dysponują niezbędnymi zasobami, aby skutecznie wdrażać SSP.

8.3.3 Komponent nr 1 SSP, polityka bezpieczeństwa Państwa, cele i zasoby, składa się z następujących elementów:

- a) podstawowa legislacja lotnicza;
- b) szczególne przepisy operacyjne;
- c) system i funkcje Państwa;
- d) wykwalifikowany personel techniczny; oraz
- e) wytyczne techniczne, narzędzia i dostarczanie informacji krytycznych dla bezpieczeństwa.

8.3.4 Podstawowa legislacja lotnicza

8.3.4.1 Wytyczne w zakresie podstawowej legislacji lotniczej (CE-1) znajdują się w Doc 9734, Część A.

Uwaga. – W niniejszym podręczniku termin „legislacja” jest używany jako termin ogólny obejmujący podstawową legislację lotniczą i szczególne przepisy operacyjne.

8.3.4.2 Może zaistnieć potrzeba ustanowienia przepisów, które upoważniają różne władze lotnicze Państwa (np. władze lotnictwa cywilnego lub komisję badania wypadków) do wykonywania swoich ról. To, czy podstawowa legislacja lotnicza musi wyraźnie wymieniać wdrażanie SSP jako jedną z ról władzy lotnictwa cywilnego, zależy od systemu prawnego Państwa. Niektóre Państwa mogą uznać, że wdrożenie SSP wiąże się z funkcjami, które zostały wymienione w ich podstawowej legislacji lotniczej. W takim przypadku, zmiana podstawowej legislacji lotniczej może nie być konieczna. Dowody na wdrożenie SSP powinny być dostępne w oficjalnych dokumentach Państwa. Państwo powinno również być w stanie wykazać swoje zaangażowanie w wypełnianie swoich obowiązków w zakresie zarządzania bezpieczeństwem, zgodnie z Załącznikiem 19.

8.3.4.3 W ramach SSP, Państwo ma ustanowić politykę egzekwowania, która:

- a) stanowi wsparcie i zachętę dla pozytywnej kultury bezpieczeństwa;
- b) opisuje sposób, w jaki Państwo zapewnia ochronę danych bezpieczeństwa i informacji bezpieczeństwa oraz związanych z nimi źródeł, zwłaszcza jeżeli przekazywane informacje są obciążające; oraz
- c) określa warunki i okoliczności, w których podmioty lotnicze posiadający SMS mogą wewnętrznie rozstrzygać o zdarzeniach związanych z pewnymi problemami związanymi z bezpieczeństwem, w kontekście ich systemów SMS i zgodnie z wymogami właściwego organu Państwa, pod warunkiem że SMS jest zgodny ze strukturą SMS oraz okazał się skuteczny i dojrzały.

8.3.4.4 Stosując zasady zarządzania bezpieczeństwem, relacje pomiędzy Państwem a podmiotami lotniczymi powinny ewoluować poza zgodność i egzekwowanie, do partnerstwa mającego na celu utrzymanie lub ciągłe podnoszenie poziomu bezpieczeństwa.

8.3.5 Szczególne przepisy operacyjne

8.3.5.1 Wytyczne w zakresie szczególnych przepisów operacyjnych (CE-2), w tym w zakresie dostosowania lub przyjęcia przepisów z innego Państwa, znajdują się w Doc 9734, Część A.

Przepisy nakazowe i oparte na wynikach

8.3.5.2 Przepisy bezpieczeństwa są ważnym narzędziem, które może być używane przez Państwa do kontrolowania ryzyka bezpieczeństwa. Wraz z przejściem do zarządzania bezpieczeństwem, pojawiła się również tendencja do wprowadzania przepisów opartych na wynikach. Aby zrozumieć, czym są przepisy oparte na wynikach, należy najpierw zrozumieć przepisy nakazowe. Przepisy nakazowe to przepisy, które wyraźnie określają, co należy zrobić i jak należy zrobić. Oczekuje się, że zapewnienie zgodności z tymi przepisami zapewni pożądany poziom bezpieczeństwa. Wiele przepisów nakazowych opracowano w następstwie wypadku i opierają się one na zdobytych doświadczeniach i chęci uniknięcia wypadku z tych samych przyczyn w przyszłości. Z punktu widzenia podmiotu lotniczego, spełnienie wymagań nakazowych wiąże się z wdrożeniem przepisów bez odstępstw. Nie oczekuje się żadnej dodatkowej analizy ani uzasadnienia ze strony podmiotu lub właściwego organu.

8.3.5.3 Do niedawna normy i zalecane metody postępowania ICAO skupiały się na wymaganiach nakazowych jako sposobie identyfikacji minimalnych standardów i zapewniania interoperacyjności. Jednak coraz częściej istnieje potrzeba posiadania przepisów opartych na wynikach w celu wsparcia innowacyjnych podejść przy wdrażaniu, które mogą poprawić skuteczność, i które mogą spełniać lub wykraczać poza cele bezpieczeństwa.

8.3.5.4 Załączniki ICAO zawierają przykłady norm, które stanowią zarówno przepisy nakazowe, jak i przepisy oparte na wynikach. Poniżej przedstawiono przykład normy z Załącznika 14 - *Lotniska*, Tom I - *Projektowanie i eksploatacja lotnisk*, która zawiera przepisy nakazowe:

3.3.1 W przypadku, gdy na końcu drogi startowej nie ma drogi kołowania umożliwiającej zjazd lub zawracanie oraz gdy literą kodu jest D, E lub F, należy zapewnić na tej drodze

startowej płaszczyznę do zawracania w celu umożliwienia samolotom wykonanie zwrotu o 180 stopni.

8.3.5.5 Powyższy przykład jest przepisem nakazowym, ponieważ określa tylko jeden sposób wykazania zgodności dla drogi startowej o określonych kryteriach: tj. zapewnienie na tej drodze startowej płaszczyzny do zawracania. Odstępstwo od przepisu nakazowego jest zazwyczaj przyznawane w drodze zwolnienia z przepisów.

8.3.5.6 Natomiast normy, które stanowią przepisy oparte na wynikach, są wyrażane w kategoriach pożądanego rezultatu. Przepisy oparte na wynikach wymagają, aby podmiot lotniczy wykazał, że proponowane przez niego podejście osiągnie pożądaną rezultat. Poniżej przedstawiono przykład normy opartej na wynikach z Załącznika 6, Część I.

7.2.11 Samolot musi być wystarczająco wyposażony w urządzenia nawigacyjne, by zapewnić, że w przypadku uszkodzenia jednego z elementów wyposażenia w dowolnej fazie lotu, pozostałe urządzenia będą zapewniać możliwość nawigacji, zgodnie z pkt 7.2.1 oraz 7.2.2, 7.2.3 i 7.2.4 tam, gdzie to ma zastosowanie.

8.3.5.7 Należy zauważyć, że powyższa norma nie wskazuje konkretnych wymaganych urządzeń nawigacyjnych. Zamiast tego opisuje pożądaną rezultat, to znaczy, że w przypadku awarii jednego elementu, pozostałe urządzenia muszą umożliwić bezpieczne nawigowanie statkiem powietrznym. Wymagane urządzenia będą zależeć od projektu statku powietrznego. Przepisy sformułowane w ten sposób będą wymagać od operatora lotniczego przedstawienia właściwemu organowi danych niezbędnych do wykazania zgodności z tym wymaganiem. Można to zrealizować za pomocą własnej analizy, ale w przypadku tego rodzaju przepisów opartych na wynikach, potrzebne informacje są często dostępne z innych źródeł. W tym przypadku zarówno właściwy organ, jak i operator, wykorzystaliby dane producentów statków powietrznych przy podejmowaniu decyzji, a operator lotniczy nie musi opracowywać własnego, nowego rozwiązania. Opracowując przepisy oparte na wynikach, Państwa muszą pamiętać, w jaki sposób można wykazać zgodność. Może zaistnieć potrzeba opracowania przez Państwo materiałów zawierających wytyczne i/lub akceptowalnych sposobów potwierdzania spełnienia wymagań w celu wsparcia branży w spełnieniu tego wymagania.

8.3.5.8 Poniżej przedstawiono inny przykład normy opartej na wynikach z Dodatku 2 do Załącznika 19.

2.1.1 Podmiot lotniczy opracowuje i utrzymuje proces, który zapewni identyfikację zagrożeń występujących w związku z oferowanymi produktami lub usługami lotniczymi.

8.3.5.9 W powyższym przykładzie, chociaż norma wymaga wprowadzenia procesu w celu identyfikacji zagrożeń, nie określa ona jak taki proces powinien wyglądać. Państwa mogą zezwolić podmiotom lotniczym na zaprojektowanie własnej metodologii. Rola organu regulacyjnego polegałaby na ocenie, czy metodologia, procesy i system ustanowione przez podmiot lotniczy prowadzą do identyfikacji zagrożeń. Organ dokonałby również oceny skuteczności procesu identyfikacji zagrożeń podmiotu, na przykład poprzez ocenę ilości, rodzajów i znaczenia zidentyfikowanych zagrożeń. Przepisy oparte na wynikach, które są sformułowane w ten sposób, wymagają od organów regulacyjnych umiejętności i specjalistycznej wiedzy do przeprowadzenia oceny działania systemu, a nie tylko oceny nakazowej zgodności z literą przepisów. Przeprowadzenie oceny wymaga również więcej zasobów, ponieważ wdrożenie może różnić się w zależności od jednego do drugiego podmiotu lotniczego.

Zapewnienie możliwości opracowania przepisów nakazowych i opartych na wynikach

8.3.5.10 W niektórych przypadkach normy i zalecane metody postępowania ICAO wymagają ustanowienia przepisów nakazowych, a jednocześnie oferują Państwom wybór ustanowienia przepisów opartych na wynikach w celu wsparcia alternatywnych sposobów spełnienia wymagań. Tam, gdzie Państwa ustanawiają możliwość opracowania przepisów zarówno nakazowych, jak i opartych na wynikach, podmioty lotnicze, które nie posiadają wiedzy specjalistycznej, aby opracować własne podejście w celu spełnienia wymagań przepisów opartych na wynikach, mogą zastosować się do przepisów nakazowych. W przypadku podmiotów, które nie posiadają takiej

wiedzy, przepisy pozwalają im na opracowanie sposobów zapewnienia zgodności odpowiednich dla ich własnych działań, a także mogą oferować zwiększoną elastyczność operacyjną i bardziej efektywne wykorzystanie zasobów. Normy dotyczące zarządzania zmęczeniem, takie jak te zawarte w Załączniku 6, Część I, zmiana nr 43, stanowi tego dobry przykład:

4.10.1 Państwo operatora ustanawia przepisy w celu zarządzania zmęczeniem. Przepisy te opierają się na zasadach naukowych, wiedzy i doświadczeniach operacyjnych w celu zapewnienia by członkowie załogi lotniczej i personelu pokładowego działali z zachowaniem odpowiedniego poziomu czujności. W związku z tym państwo operatora ustala:

- a) przepisy dotyczące ograniczeń czasu lotu, okresu pełnienia czynności lotniczych, okresu służby i czasu odpoczynku; oraz*
- b) przepisy FRMS, jeżeli operator, w celu zarządzania zmęczeniem, uprawniony jest do wprowadzenia systemu zarządzania ryzykiem związanym ze zmęczeniem (FRMS).*

4.10.2 Państwo operatora wymaga od operatora, zgodnie z pkt 4.10.1, oraz w celu zarządzania ryzykiem związanym z ryzykiem dla zmęczenia, ustanowienia:

- a) ograniczenia czasu lotu, okresu pełnienia czynności lotniczych, okresu służby i czasu odpoczynku, zgodne z zapisami dotyczącymi zarządzania zmęczeniem ustanowionymi przez państwo operatora; lub*
- b) System zarządzania ryzykiem związanym ze zmęczeniem (FRMS) zgodny z zapisami zawartymi w pkt 4.10.6 do wszystkich operacji; lub*
- c) c) system FRMS zgodny z zapisami pkt 4.10.6 dla części operacji oraz wymagań określonych w pkt 4.10.2 a) dla pozostałych operacji.*

8.3.5.11 W powyższym przykładzie norma wymaga od Państw ustanowienia nakazowych przepisów dotyczących ograniczenia czasu lotu i okresu służby, natomiast ustanowienie przepisów dotyczących FRMS jest opcjonalne. FRMS daje operatorowi lotniczemu możliwość lepszego odniesienia się do specyficznych ryzyk związanych ze zmęczeniem, a jednocześnie oferuje możliwość elastyczności operacyjnej poza nakazowymi przepisami dotyczącymi ograniczenia czasu lotu i okresu służby. Państwo musi rozważyć, czy oprócz obowiązkowych przepisów nakazowych w zakresie ograniczeń, konieczne jest zapewnienie, alternatywnie, przepisów w zakresie FRMS oraz czy posiada ono niezbędne zasoby do zapewnienia odpowiedniego nadzoru nad FRMS. Następnie norma 4.10.2 wyjaśnia, że operatorzy lotniczy są zobowiązani do zarządzania ryzykiem bezpieczeństwa związanym ze zmęczeniem. W przypadku ustanowienia przepisów FRMS można to zapewnić w ramach nakazowych przepisów o ograniczeniach, o których mowa w pkt 4.10.2 (a), lub poprzez wdrożenie FRMS opartego na wynikach, o którym mowa w pkt 4.10.2 (b) i (c). Operatorzy, którzy nie posiadają wiedzy specjalistycznej, aby opracować FRMS i spełnić związane z tym wymagania przepisów, musieliby przestrzegać przepisów nakazowych.

8.3.5.12 Oczywiście powinno być, że przepisy oparte na wynikach nie zawsze są odpowiednie. Wymagania nakazowe są odpowiednie, gdy konieczne są znormalizowane sposoby zapewniania zgodności, na przykład w celu ułatwienia interoperacyjności. Dla przykładu, wymagania dotyczące oznakowania poziomego drogi startowej są z natury rzeczy nakazowe.

8.3.5.13 W praktyce przepisy rzadko są w pełni nakazowe lub w pełni oparte na wynikach, ale zawierają elementy jednych i drugich przepisów. Są również w różnym stopniu oparte na wynikach. Kiedy Państwo rozważy wdrożenie przepisów opartych na wynikach, musi wziąć pod uwagę możliwości i dojrzałość branży, konkretnych jej sektorów, a nawet dojrzałość poszczególnych podmiotów lotniczych i ich systemów zarządzania bezpieczeństwem. Przepisy oparte na wynikach nakładają również większe wymagania na organ regulacyjny, wymagając nie tylko

sprawdzenia zgodności, ale także oceny systemów i poziomu bezpieczeństwa z uwzględnieniem specyficznego kontekstu operacyjnego każdego podmiotu lotniczego. Państwa muszą zagwarantować, że będą w stanie nadzorować branżę i nią zarządzać, biorąc pod uwagę, że wymagany będzie zarówno wyższy poziom wiedzy specjalistycznej, jak i większe zasoby. System SMS stanowi podstawę oraz zapewnia narzędzia dla podmiotów lotniczych umożliwiające przestrzeganie przepisów opartych na wynikach, jednak nie sprowadza się to do automatycznego zapewnienia, że każdy podmiot posiadający SMS ma możliwość aby je zrealizować. Zależy to od wymagań określonych przepisów opartych na wynikach.

8.3.5.14 Przepisy oparte na wynikach mają również wpływ na egzekwowanie. Egzekwowanie przepisów nakazowych jest proste, ponieważ niezgodność można łatwo określić. Egzekwowanie jest trudniejsze w przypadku przepisów opartych na wynikach. Na przykład podmiot lotniczy może wykazać, że ma wdrożony proces, który spełnia przepisy (na przykład posiada system zgłaszania zagrożeń), ale nie jest w stanie wykazać, że proces zapewnia zamierzony rezultat (na przykład, czy system zgłaszania zagrożeń jest skuteczny). Może to prowadzić do ustanowienia systemów lub procesów, które jedynie spełniają „literę prawa”, ale nie zapewniają wymaganego rezultatu związanego z bezpieczeństwem. Organy regulacyjne mogą być zmuszone do zaangażowania odpowiednich organów egzekwowania prawa w opracowanie przepisów opartych na wynikach w celu zapewnienia ich egzekwowalności.

8.3.6 System i funkcje Państwa

8.3.6.1 Wytyczne w zakresie systemu i funkcji Państwa (CE-3) znajdują się w Doc 9734, Część A.

Organizacja odpowiedzialna za koordynację SSP

8.3.6.2 Obowiązki Państwa związane z zarządzaniem bezpieczeństwem mogą być realizowane przez wiele władz lotniczych Państwa, na przykład władzę lotnictwa cywilnego i niezależną komisję badania wypadków. Państwa powinny wyjaśnić, który organ w Państwie jest odpowiedzialny za koordynację działań w zakresie utrzymania i wdrażania SSP. Wiele Państw przypisuje tę rolę władzy lotnictwa cywilnego, biorąc pod uwagę, że jest ona zazwyczaj odpowiedzialna za większość obowiązków związanych z SSP. Role i obowiązki wszystkich zaangażowanych organów powinny zostać określone i udokumentowane.

Grupa koordynacyjna SSP

8.3.6.3 Państwo powinno ustanowić odpowiednią grupę koordynacyjną składającą się z przedstawicieli zaangażowanych władz lotniczych, których obowiązki związane są z wdrażaniem i utrzymaniem SSP, w tym przedstawicieli komisji badania wypadków, a także przedstawicieli wojskowych władz lotniczych. Powołanie grupy koordynacyjnej ułatwi dobrą komunikację, pozwoli uniknąć powielania wysiłków i prowadzenia sprzecznych polityk oraz zapewni skuteczne wdrożenie SSP. Grupa ta jest formą komitetu pod przewodnictwem szefa organizacji odpowiedzialnej za koordynację działań w ramach SSP.

8.3.6.4 Państwo może również uznać za korzystne przydzielanie codziennego planowania oraz zarządzania wdrożeniem SSP osobie, wydziałowi lub zespołowi. Taka osoba, wydział lub zespół mogą zapewnić, że różne aspekty współpracują ze sobą w celu osiągnięcia celów bezpieczeństwa Państwa.

Funkcje i działania związane z SSP

8.3.6.5 Sposób, w jaki Państwa decydują się zorganizować swoją siłę roboczą i strukturę organizacyjną w zakresie monitorowania wdrożenia systemu zarządzania bezpieczeństwem przez podmioty lotnicze zgodnie z Załącznikiem 19, leży w gestii każdego Państwa. Państwo może zdecydować się na powołanie nowej komórki lub dodać tę odpowiedzialność do zakresu obowiązków istniejących komórek, na przykład: departamentu techniki lotniczej, departamentu operacyjno-lotniczego, departamentu żeglugi powietrznej i departamentu lotnisk, itp. Decyzja będzie zależała od tego, w jaki sposób Państwo zdecyduje się wdrożyć wymagania w zakresie nowych kompetencji.

8.3.6.6 Ważne jest, aby różne władze lotnicze miały jasność co do swojej roli. Powinno to dotyczyć wszystkich ich obowiązków, funkcji i działań związanych z SSP. Państwo powinno zapewnić, że każdy organ rozumie swój wkład w realizację poszczególnych wymagań Załącznika 19, a co najważniejsze, swoją odpowiedzialność za zarządzanie bezpieczeństwem Państwa. Zobowiązania i funkcje każdej władzy lotniczej w odniesieniu do wdrożenia SSP powinny być udokumentowane w celu uniknięcia dwuznaczności.

8.3.6.7 Powinny istnieć odpowiednie struktury zarządzania w Państwach, w których personel zaangażowany w bezpieczeństwo jest rozproszony pod względem geograficznym. Złożona struktura zarządzania może nie być konieczna w przypadku mniej skomplikowanych systemów lotniczych, gdzie niewiele osób jest zaangażowanych w zarządzanie bezpieczeństwem. Państwo powinno zapewnić, aby cały personel miał to samo zrozumienie wdrożenia SSP na poziomie krajowym. Podejście do wdrożenia SSP powinno być udokumentowane.

Polityka bezpieczeństwa i cele bezpieczeństwa Państwa

8.3.6.8 Skuteczne wdrożenie SSP wymaga zaangażowania ze strony kierownictwa wyższego szczebla oraz wsparcia ze strony personelu na wszystkich szczeblach. Polityka bezpieczeństwa Państwa i cele bezpieczeństwa Państwa to oświadczenia wysokiego szczebla zatwierdzone przez władze lotnicze Państwa. W połączeniu kierują one zachowaniem w zakresie bezpieczeństwa i alokacją zasobów. Polityka i cele bezpieczeństwa Państwa powinny być publikowane i poddawane okresowym przeglądom w celu zapewnienia, że są one aktualne i odpowiednie dla Państwa.

Polityka bezpieczeństwa Państwa

8.3.6.9 Zobowiązanie kierownictwa wyższego szczebla powinno być wyrażone w polityce bezpieczeństwa Państwa. Polityka bezpieczeństwa Państwa jest formalnym dokumentem opisującym intencje i kierunek działań Państwa w zakresie bezpieczeństwa. Polityka bezpieczeństwa Państwa określa podejście kierownictwa wyższego szczebla do bezpieczeństwa i promowania pozytywnej kultury bezpieczeństwa w Państwie. Można ją uznać za oświadczenie w sprawie misji i wizji bezpieczeństwa Państwa.

8.3.6.10 Polityka bezpieczeństwa powinna odnosić się do kluczowych praktyk, które są niezbędne do zarządzania bezpieczeństwem oraz do sposobu, w jaki kierownictwo wyższego szczebla planuje wypełniać swoje obowiązki w zakresie bezpieczeństwa (np. zastosowanie podejścia w oparciu o dane). Zasady odzwierciedlone w polityce bezpieczeństwa powinny być wyraźnie widoczne w codziennych praktykach Państwa.

8.3.6.11 Polityka bezpieczeństwa Państwa jest zatwierdzana przez władze lotnicze Państwa w celu wykazania swoich intencji związanych z bezpieczeństwem oraz jest realizowana jako procedura lub protokół. Typowe oświadczenie to: „Osiągniemy bezpieczeństwo poprzez: (1) akceptację odpowiedzialności za bezpieczne warunki i zachowania (2) kulturę przywództwa w zakresie bezpieczeństwa, współpracę, otwartą komunikację itp.”

Cele bezpieczeństwa Państwa

8.3.6.12 Opracowanie celów bezpieczeństwa rozpoczyna się od jednoznacznego zrozumienia największych ryzyk bezpieczeństwa w systemie lotniczym. Na ryzyko bezpieczeństwa w systemie lotniczym wpływa wiele różnych czynników, takich jak wielkość i złożoność systemu lotniczego oraz środowisko operacyjne. Opracowanie dobrego opisu systemu zapewni dobre wprowadzenie i zrozumienie. Patrz pkt 8.7 niniejszego rozdziału w zakresie wdrożenia SSP.

8.3.6.13 W celu zrozumienia głównych ryzyk bezpieczeństwa należy, w miarę możliwości, wykorzystywać dane ilościowe. Państwo może również wykorzystywać informacje jakościowe i analizy ekspertów. Można utworzyć grupę wybranych ekspertów prowadzących dyskusje mające zapewnić szersze zrozumienie ryzyk bezpieczeństwa w systemie lotniczym. Grupa taka miałaby podobną rolę jak Komisja ds. przeglądu bezpieczeństwa (SRB), jak omówiono w Rozdziale 9, pkt 9.3.6; w tym przypadku na poziomie Państwa. Kierunki prac ekspertów wynikałyby z dostępnych informacji o trendach w zakresie bezpieczeństwa, czynników sprawczych znanych wypadków i

poważnych incydentów lub wiadomych niedociągnięć w procesach krajowego nadzoru na bezpieczeństwem. Praca ekspertów można również uwzględniać cele regionalne lub cele globalne określone w GASP. Podejście typu „burza mózgów” może być realizowane wspólnie z podmiotami lotniczymi w celu identyfikacji znanych problemów związanych z bezpieczeństwem w każdym sektorze lotnictwa.

8.3.6.14 Cele bezpieczeństwa Państwa to krótkie oświadczenia wysokiego szczebla, które wytyczają kierunek działań dla wszystkich właściwych organów Państwa. Stanowią one pożądane wyniki bezpieczeństwa, które Państwo chce osiągnąć. Przy określaniu celów bezpieczeństwa ważne jest również wzięcie pod uwagę zdolności Państwa do wpływania na pożądane wyniki. Cele bezpieczeństwa reprezentują priorytety Państwa w zakresie zarządzania bezpieczeństwem i stanowią plan przydzielania i kierowania zasobami Państwa.

8.3.6.15 Cele bezpieczeństwa wspierają identyfikację wskaźników SPI i poziomów SPT oraz późniejsze ustalenie akceptowalnego poziomu bezpieczeństwa (ALoSP), omówionego w dalszej części niniejszego Rozdziału. Cele bezpieczeństwa współpracują ze sobą jako pakiet z SPI i SPT, aby umożliwić Państwu monitorowanie i pomiar poziomu bezpieczeństwa. Dalsze wytyczne dotyczące SPI i SPT znajdują się w Rozdziale 4.

8.3.6.16 Po wdrożeniu SSP, Państwo powinno okresowo oceniać zidentyfikowane ryzyka bezpieczeństwa, analizując informacje bezpieczeństwa wygenerowane przez SSP. Analiza pomoże również zidentyfikować pojawiające się problemy. Wytyczne dotyczące analizy bezpieczeństwa znajdują się w Rozdziale 6. Państwo powinno również okresowo dokonywać przeglądu swoich postępów w osiąganiu celów bezpieczeństwa i ich ciągłej adekwatności, pamiętając o wszelkich ponownych ocenach obecnego ryzyka.

Zasoby bezpieczeństwa Państwa

8.3.6.17 Państwo musi zapewnić, aby instytucje, które posiadają przypisane obowiązki w zakresie bezpieczeństwa, dysponowały wystarczającymi zasobami do wykonywania swoich zadań. Dotyczy to zarówno zasobów finansowych, jak i zasobów ludzkich.

8.3.6.18 Niektóre władze lotnicze są finansowane w oparciu o budżet przydzielony przez Państwo. Inne są finansowane z opłat pobieranych od stron uczestniczących w systemie lotniczym (np. opłaty za licencje i zatwierdzenia) lub od stron korzystających z usług systemu lotniczego (np. opłaty od pasażerów lub za paliwo). Źródło finansowania, które jest najbardziej odpowiednie dla Państwa, zależy od okoliczności, w jakich Państwo to funkcjonuje. Na przykład Państwo, które posiada małą branżę lotniczą, może uznać, że jego władza lotnictwa cywilnego nie może polegać wyłącznie na opłatach finansujących działania prawodawcze. Państwo może potrzebować wielu źródeł finansowania działalności lotniczej.

8.3.6.19 W miarę jak Państwo zaczyna w pełni realizować SSP i stosować praktyki zarządzania bezpieczeństwem, może się okazać, że konieczne jest ponowne sprawdzenie budżetu i finansowania w celu zapewnienia, że posiada wystarczający strumień dochodów. Nowe funkcje są wprowadzane i będą musiały być wykonane dobrze, aby podejście przyjęte w zarządzaniu bezpieczeństwem odniosło sukces, w tym na przykład w zakresie zarządzania ryzykiem bezpieczeństwa, zbierania i analizy danych oraz promocji bezpieczeństwa. Zarządzanie bezpieczeństwem wymaga również od władz lotniczych Państwa ciągłego monitorowania i przeglądu własnych procesów zarządzania ryzykiem bezpieczeństwa. Inspektorzy oraz pozostały personel mogą potrzebować przekwalifikowania. W związku z tym Państwo może uznać za konieczne przeznaczenie wystarczających środków finansowych na rzecz agencji państwowych w momencie przejścia na podejście do zarządzania bezpieczeństwem.

Krajowy plan bezpieczeństwa lotniczego (NASP)

8.3.6.20 Rezolucja Zgromadzenia A39-12 ICAO w sprawie globalnego planowania w zakresie bezpieczeństwa i żeglugi powietrznej wskazuje na znaczenie skutecznego wdrożenia krajowych planów bezpieczeństwa lotniczego. Określa, że Państwa powinny opracować i wdrożyć krajowe plany bezpieczeństwa lotniczego, zgodnie z celami Globalnego planu bezpieczeństwa lotniczego (GASP, Doc 10004). Na poziomie

międzynarodowym, GASP określa strategię, która wspiera wyznaczanie priorytetów i ciągłe doskonalenie bezpieczeństwa lotniczego. Regionalne i krajowe plany bezpieczeństwa lotniczego powinny być opracowywane zgodnie z GASP.

8.3.6.21 Na poziomie regionalnym, proces planowania jest koordynowany przez regionalne grupy ds. bezpieczeństwa lotniczego (RASG). Regionalne i krajowe inicjatywy na rzecz poprawy bezpieczeństwa (SEI) powinny zostać odpowiednio dostosowane w oparciu o kwestie, w obliczu których stoją zainteresowane Państwa. Krajowy plan bezpieczeństwa lotniczego przedstawia strategiczny kierunek zarządzania bezpieczeństwem lotniczym na poziomie krajowym na czas określony (np. w ciągu najbliższych pięciu lat). Wskazuje on wszystkim zainteresowanym stronom obszary, w obrębie których władze lotnicze Państwa powinny koncentrować swoje wysiłki w nadchodzących latach.

8.3.6.22 Krajowy plan bezpieczeństwa lotniczego pozwala Państwu jednoznacznie zakomunikować swoją strategię na rzecz poprawy bezpieczeństwa na poziomie krajowym wszystkim zainteresowanym stronom, w tym innym jednostkom administracji rządowej oraz pasażerom. Stanowi on środek służący ujawnieniu sposobu, w jaki władza lotnictwa cywilnego i inne podmioty lotnicze będą pracować nad identyfikacją zagrożeń i zarządzaniem ryzykiem bezpieczeństwa operacyjnego oraz nad innymi problemami związanymi z bezpieczeństwem. Pokazuje również, w jaki sposób planowane inicjatywy na rzecz poprawy bezpieczeństwa pomogą Państwu w osiągnięciu ustalonych celów. Krajowy plan bezpieczeństwa lotniczego podkreśla zaangażowanie Państwa w bezpieczeństwo lotnicze.

8.3.6.23 Każde Państwo powinno opracować krajowy plan bezpieczeństwa lotniczego. Jeżeli Państwo posiada już krajowy program bezpieczeństwa (SSP), krajowy plan bezpieczeństwa lotniczego może zostać uwzględniony w komponencie nr 1: polityka bezpieczeństwa Państwa, cele i zasoby. Krajowy plan bezpieczeństwa lotniczego może zostać opublikowany jako oddzielny dokument wysokiego szczebla w celu ułatwienia komunikacji z opinią publiczną i innymi podmiotami zewnętrznymi w stosunku do władzy lotnictwa cywilnego.

Dokumentacja SSP

8.3.6.24 Państwo powinno opisać swój krajowy program bezpieczeństwa w postaci dokumentu w celu zapewnienia, że cały zainteresowany personel ma wspólne zrozumienie w tym zakresie. Dokument powinien przedstawiać strukturę programu i programy powiązane, sposób w jaki poszczególne elementy współpracują ze sobą, a także role różnych władz lotniczych Państwa. Dokumentacja powinna stanowić uzupełnienie istniejących procesów i procedur oraz szeroko opisywać sposób, w jaki różne programy podporządkowane SSP współpracują ze sobą w celu poprawy bezpieczeństwa. W dokumentacji pomocniczej można również uwzględnić odniesienia do zakresu obowiązków i odpowiedzialności poszczególnych organów w zakresie bezpieczeństwa. Państwo powinno wybrać sposób dokumentowania i rozpowszechniania informacji, który najlepiej służyłby jego środowisku, na przykład w postaci fizycznego dokumentu lub na odpowiednio kontrolowanej stronie internetowej. Niezależnie od wybranego kanału komunikacji, podejmowane działania mają na celu ułatwienie wspólnego rozumienia SSP wśród całego zainteresowanego personelu.

8.3.7 Wykwalifikowany personel techniczny

8.3.7.1 Wytyczne w zakresie wykwalifikowanego personelu technicznego wykonującego funkcje związane z bezpieczeństwem (CE-4) znajdują się w Doc 9734, Część A.

Ogólne wytyczne

8.3.7.2 Państwa będą musiały zidentyfikować i zająć się kompetencjami wymaganymi do skutecznego wdrożenia SSP, biorąc pod uwagę role i obowiązki w ramach SSP wykonywane przez ich personel.

Kompetencje te stanowią uzupełnienie kompetencji wymaganych do prowadzenia nadzoru zgodności i mogą być zapewniane poprzez szkolenie obecnych pracowników lub zatrudnianie dodatkowego personelu, i obejmują między innymi:

- a) zwiększone umiejętności przywódcze;
- b) zrozumienie procesów biznesowych;
- c) doświadczenie i osąd wymagane do oceny wyników i skuteczności;
- d) nadzór oparty na ryzyku bezpieczeństwa;
- e) zbieranie i analizę danych bezpieczeństwa;
- f) pomiar i monitorowanie poziomu bezpieczeństwa; oraz
- g) działania promujące bezpieczeństwo.

8.3.7.3 Wytyczne w zakresie rozwoju i utrzymania efektywnego personelu inspektorskiego znajdują się w *Podręczniku kompetencji inspektorów bezpieczeństwa lotnictwa cywilnego* (Doc 10070).

8.3.7.4 Państwo powinno określić najbardziej odpowiednie szkolenia dla personelu pełniącego różne role i obowiązki w organizacji. Oto przykłady szkoleń, które należy wziąć pod uwagę:

- a) briefingi lub szkolenia zapoznawcze dla kierownictwa wyższego szczebla na temat krajowego programu bezpieczeństwa (SSP), systemu zarządzania bezpieczeństwem (SMS), polityki i celów bezpieczeństwa oraz akceptowalnego poziomu bezpieczeństwa (ALoSP);
- b) szkolenie inspektorów w zakresie zasad SSP i SMS, sposobu prowadzenia oceny SMS, sposobu oceny wskaźników SPI podmiotu lotniczego pod kątem akceptacji oraz w zakresie sprawowania ogólnego nadzoru nad podmiotem w środowisku zarządzania bezpieczeństwem;
- c) szkolenie w zakresie umiejętności miękkich (skuteczne umiejętności komunikacyjne, umiejętności negocjacyjne, rozwiązywanie konfliktów, itp.) w celu wsparcia inspektorów we współpracy z podmiotami lotniczymi w celu poprawy poziomu bezpieczeństwa przy jednoczesnym zapewnieniu ciągłej zgodności z ustanowionymi przepisami;
- d) szkolenie personelu odpowiedzialnego za analizę danych, cele bezpieczeństwa, SPI i SPT;
- e) szkolenia dla lekarzy orzeczników medycyny lotniczej i asesorów medycznych;
- f) ochrona danych bezpieczeństwa, informacji bezpieczeństwa i powiązanych źródeł oraz szkolenie w zakresie polityki egzekwowania przepisów dla personelu prawnego, itp.; oraz
- g) szkolenie w zakresie SSP i SMS dla osób prowadzących badanie bezpieczeństwa podmiotu lotniczego.

8.3.7.5 Programy szkolenia w zakresie bezpieczeństwa dla personelu zaangażowanego w obowiązki związane z SSP powinny być odpowiednio koordynowane pomiędzy instytucjami Państwa. Zakres szkolenia lub znajomości SSP i SMS powinien odzwierciedlać rzeczywiste procesy SSP i sam SSP w miarę jego ewoluowania i dojrzewania. Początkowe szkolenie SSP i SMS może być ograniczone do ogólnych elementów SSP lub elementów struktury SMS.

8.3.7.6 W celu zapewnienia, że cały zainteresowany personel techniczny jest odpowiednio wykwalifikowany, Państwo powinno:

- a) opracować wewnętrzne polityki i procedury szkolenia; oraz
- b) opracować program szkolenia w zakresie SSP i SMS dla zainteresowanych pracowników. Pierwszeństwo należy nadać personelowi odpowiedzialnemu za wdrożenie SSP/SMS oraz inspektorom operacyjnym zaangażowanym w nadzór/monitorowanie SMS podmiotów lotniczych; (w tym specyficzne dla Państwa procesy SSP i ich znaczenie).

8.3.7.7 Dostępnych jest wiele różnych rodzajów szkoleń w zakresie SSP i SMS, w tym kursy online, kursy w klasie, warsztaty, itp. Rodzaj i ilość oferowanych szkoleń powinny zapewnić, że zainteresowany personel rozwinie kompetencje potrzebne do wykonywania swoich funkcji oraz zrozumie swój wkład w SSP. Działania te mają na celu upewnienie się, że osoba lub zespół zajmują się każdym aspektem SSP oraz że zostali oni przeszkoleni do wykonywania przydzielonych funkcji.

8.3.7.8 Odpowiednie i wystarczające szkolenia dla inspektorów zapewnią spójny nadzór i wymagane zdolności w celu uzyskania skuteczności w środowisku zarządzania bezpieczeństwem. Państwa powinny rozważyć następujące kwestie:

- a) Nadzór i monitorowanie systemu SMS podmiotów lotniczych będą wymagać kompetencji, które mogły nie być określane jako krytyczne przed wprowadzeniem wymagań związanych z SMS. Inspektorzy będą musieli uzupełnić swoją istniejącą wiedzę techniczną dodatkowymi umiejętnościami polegającymi na ocenie przydatności i skuteczności wdrożenia systemu SMS przez podmioty lotnicze. Takie podejście wymaga współpracy z branżą, zdobycia zaufania podmiotów w celu ułatwienia udostępniania danych bezpieczeństwa i informacji bezpieczeństwa. Państwa będą musiały zapewnić odpowiednie szkolenie w celu zapewnienia, że personel odpowiedzialny za współdziałanie z branżą posiada kompetencje i elastyczność w wykonywaniu działań nadzorczych w środowisku SMS. Analiza potrzeb szkoleniowych może być wykorzystana do identyfikacji odpowiednich szkoleń.
- b) Szkolenie powinno również zapewniać pracownikom świadomość roli i wkładu wnoszonego przez inne komórki w obrębie ich władzy lotniczej i innych władz lotniczych Państwa. Zapewni to, że zarówno inspektorzy, jak i personel z innych władz lotniczych Państwa, posiada takie samo spójne podejście. Ułatwi to również lepsze zrozumienie ryzyk bezpieczeństwa w różnych sektorach. Inspektorzy mogą również lepiej zrozumieć, w jaki sposób przyczyniają się do osiągnięcia celów bezpieczeństwa Państwa.

8.3.8 Wytyczne techniczne, narzędzia i dostarczanie informacji krytycznych dla bezpieczeństwa

8.3.8.1 Wytyczne w zakresie wytycznych technicznych, narzędzi i dostarczania informacji krytycznych dla bezpieczeństwa (CE-5) znajdują się w Doc 9734, Część A.

8.3.8.2 Państwo powinno uwzględnić zapewnienie wytycznych dla swoich inspektorów oraz podmiotów lotniczych w celu zapewnienia pomocy w interpretacji przepisów dotyczących zarządzania bezpieczeństwem. Działania takie będą promować pozytywną kulturę bezpieczeństwa i pomogą podmiotom w osiągnięciu ich celów bezpieczeństwa, a co za tym idzie, celów bezpieczeństwa Państwa, które często są osiąganane poprzez regulację. Ocena systemów SMS może wymagać dodatkowych narzędzi do określenia zgodności i wydajności systemu SMS podmiotów lotniczych. Przed ich wdrożeniem, wszelkie opracowane narzędzia będą wymagały przeszkolenia personelu, którego bezpośrednio dotyczą.

8.4. KOMPONENT NR 2: ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA PRZEZ PAŃSTWO

8.4.1 Państwa muszą zidentyfikować potencjalne ryzyka bezpieczeństwa dla systemu lotniczego. Państwo powinno wzmocnić swoje tradycyjne metody analizowania przyczyn wypadku lub incydentu poprzez zastosowanie proaktywnych procesów. Proaktywne procesy umożliwiają Państwu identyfikację i odniesienie do czynników prekursorowych i sprawczych wypadków oraz strategiczne zarządzanie zasobami bezpieczeństwa w celu maksymalnej poprawy bezpieczeństwa. Państwa powinny:

- a) wymagać, aby podmioty lotnicze wdrożyły system SMS w celu zarządzania i poprawy bezpieczeństwa działań związanych z lotnictwem;
- b) ustanowić środki w celu określenia czy zarządzanie ryzykiem bezpieczeństwa (SRM) przez podmioty lotnicze jest akceptowalne; oraz
- c) prowadzić przegląd i upewniać się, że system SMS podmiotu jest skuteczny.

8.4.2 Komponent SRM obejmuje wdrażanie systemu SMS przez podmioty lotnicze, w tym procesy identyfikacji zagrożeń i zarządzanie powiązаныmi ryzykami bezpieczeństwa.

8.4.3 Państwa powinny również stosować zasady SRM do swoich własnych działań. Dotyczy to takich działań jak opracowywanie przepisów i ustalanie priorytetów działań nadzorczych w oparciu o oszacowane ryzyko.

8.4.4 Obszarem często pomijanym przez podmioty lotnicze i regulatorów jest ryzyko bezpieczeństwa wywołane przez interfejsy z innymi podmiotami. Interfejs pomiędzy SSP a SMS może stanowić szczególne wyzwanie dla Państw i podmiotów. Państwo powinno uwzględnić podkreślenie znaczenia zarządzania ryzykiem interfejsów SMS poprzez swoje przepisy i wytyczne. Przykłady ryzyka dotyczącego interfejsu to:

- a) Zależność - organizacja A jest uzależniona od organizacji B w zakresie dostarczania towarów lub usług. Organizacja B nie ma jasności co do oczekiwań i zależności organizacji A i nie udaje się jej zrealizować swoich zadań.
- b) Kontrola - organizacje współpracujące często mają minimalną kontrolę nad jakością lub skutecznością organizacji współpracującej (-ych).

8.4.5 W obu tych przypadkach zarządzanie ryzykiem dotyczącym interfejsu może wskazać na ryzyko, wyjaśnić wzajemne oczekiwania i złagodzić niepożądane konsekwencje poprzez wzajemnie uzgodnione kontrole elementów granicznych. Dodatkowe informacje na temat interfejsów pomiędzy podmiotami lotniczymi znajdują się w Rozdziale 2.

8.4.6 Obowiązki licencjonowania, certyfikacji, upoważniania i zatwierdzania

8.4.6.1 Wytyczne w zakresie obowiązków licencjonowania, certyfikacji, upoważniania i zatwierdzania (CE-6) znajdują się w Doc 9734, Część A.

8.4.6.2 Obowiązki licencjonowania, certyfikacji, upoważniania i zatwierdzania są ważnymi elementami strategii kontroli ryzyka bezpieczeństwa Państwa. Zapewniają one Państwu pewność, że podmioty lotnicze i inne właściwe organizacje reprezentujące branżę osiągnęły wymagane standardy bezpiecznego działania w systemie lotniczym. Niektóre Państwa ustanowiły wspólne przepisy operacyjne w celu ułatwienia uznawania lub akceptacji licencji, certyfikatów, upoważnień i zatwierdzeń wydanych przez inne Państwa. Takie ustalenia nie zwalniają Państwa z obowiązków wynikających z Konwencji chicagowskiej.

8.4.7 Obowiązki związane z systemem zarządzania bezpieczeństwem

Wymagania dotyczące działań regulacyjnych w zakresie SMS

8.4.7.1 Zgodnie z Załącznikiem 19, Państwo wymaga od podmiotów lotniczych i międzynarodowych operatorów lotnictwa ogólnego wdrożenia systemu zarządzania bezpieczeństwem. Wymagania odnoszą się do struktury SMS znajdującej się w Załączniku 19, Dodatek 2 oraz do wytycznych zawartych w Rozdziale 9 niniejszego podręcznika. Sposób ustanowienia tych wymagań będzie zależał od ram prawnych danego Państwa.

8.4.7.2 Państwa powinny ustanowić proces zapewniający, że SMS jest akceptowany przez Państwo. Jedno podejście to ustalanie terminów i kamieni milowych na poziomie Państwa, które reprezentują wymagany postęp we wdrażaniu SMS. Dodatkowe wytyczne dla podmiotów lotniczych dotyczące sposobu opracowania i wykonania analizy luk oraz planu wdrożenia SMS znajdują się w Rozdziale 9.

8.4.7.3 Wymagania dotyczące działań regulacyjnych w zakresie SMS i materiały zawierające wytyczne z zakresu SMS powinny być okresowo poddawane przeglądom. Przegląd powinien uwzględniać opinie branżowe, okresowy przegląd profilu ryzyka bezpieczeństwa, aktualny status i zastosowanie norm i zalecanych metod postępowania ICAO w zakresie SMS oraz materiałów zawierających wytyczne.

Międzynarodowe lotnictwo ogólne

8.4.7.4 Przepisy w zakresie SMS dla międzynarodowego lotnictwa ogólnego (IGA) znajdują się z pewnym elementem elastyczności w Załączniku 19 i dlatego nie są uwzględniane w wykazie podmiotów lotniczych. Oczekuje się, że ten sektor lotnictwa również wdroży strukturę SMS. Różnica pomiędzy tym a innymi sektorami polega na tym, że w tym przypadku Państwa mają pewien stopień elastyczności w określaniu wymagań. Zgodnie z innymi przepisami zawartymi w Załączniku 6, Część II – *Międzynarodowe lotnictwo ogólne – Samoloty*, Państwo rejestracji ustanawia kryteria dla operatorów międzynarodowego lotnictwa ogólnego do wdrożenia SMS.

8.4.7.5 Ustalenie kryteriów powinno wymagać zastosowania struktury SMS zgodnie z opisem znajdującym się w Załączniku 19, ale można to osiągnąć na wiele sposobów:

- a) kryteria są ustalane w ramach istniejących szczególnych przepisów operacyjnych dotyczących międzynarodowego lotnictwa ogólnego;
- b) publikacja wymogów w ramach struktury przepisów prawnych w instrumencie prawnym innym niż szczególne przepisy operacyjne, które określają kryteria; lub
- c) dokonywanie odniesień w ramach struktury przepisów prawnych do kodeksu praktyk branżowych SMS uznanych przez Państwo.

8.4.7.6 Wybierając najlepsze podejście do ustanowienia kryteriów SMS dla międzynarodowego lotnictwa ogólnego, Państwo rejestracji powinno rozważyć, w jaki sposób będzie prowadzone monitorowanie SMS, w tym ewentualne przekazanie nadzoru stronie trzeciej. Podobnie jak w przypadku systemu SMS podmiotów lotniczych, przy określaniu akceptowalności systemu SMS, Państwo rejestracji powinno pozwolić na skalowalność w oparciu o rozmiar, środowisko operacyjne i złożoność operacji.

8.4.7.7 W przypadku dużych lub turboodrzuć statków powietrznych w wielu Państwach rejestracji, które otrzymały certyfikat przewoźnika lotniczego (AOC) zgodnie z Załącznikiem 6, Część I, operator zostałby uznany za podmiot lotniczy i traktowany jako posiadający system SMS, który musi być zaakceptowany przez Państwo operatora.

Akceptacja SMS

8.4.7.8 Wiele podmiotów lotniczych posiada certyfikaty, upoważnienia lub zatwierdzenia z więcej niż jednego Państwa lub prowadzi operacje w więcej niż jednym Państwie. Załącznik 19 nie zawiera wymagania dotyczącego sprawowania nadzoru systemu SMS podmiotu lotniczego, znajdującego się poza zakresem odpowiedzialności Państwa. Jednak harmonizacja wymagań w zakresie SMS ułatwia akceptację systemów SMS pomiędzy poszczególnymi Państwami. Harmonizacja ogranicza powielanie działań nadzorczych i konieczność spełnienia przez podmioty lotnicze podobnych obowiązków w zakresie SMS poprzez (potencjalnie) odmienne wymagania. Państwa powinny być świadome polityki, która zwiększa obciążenia administracyjne i finansowe dla posiadaczy certyfikatów nie dając widocznych korzyści związanych z bezpieczeństwem. Co ważne, w przypadku podmiotów lotniczych, które nie korzystają ze wspólnej akceptacji ich certyfikatów, upoważnień lub zatwierdzeń, wprowadzenie systemu SMS pogorszyło sytuację. Państwa powinny starać się osiągnąć korzyści z wdrożenia bez nakładania dodatkowych nadmiernych obciążeń na podmioty lotnicze.

8.4.7.9 Ponadto zachęca się Państwa do stosowania w równym stopniu wymogów przy przyznawaniu certyfikatów, upoważnień lub zatwierdzeń podmiotom lotniczym innych Państw, bez nadmiernych obciążeń technicznych, prawnych i administracyjnych. Wiele podmiotów lotniczych potrzebuje dodatkowych zasobów do wstępnej akceptacji przez wiele Państw oraz do wsparcia okresowego monitorowania lub audytów z Państw, które zaakceptowały ich system SMS. Dodatkowy wysiłek jest również wymagany kiedy wymagania są różne, kiedy są różnie interpretowane lub kiedy są sprzeczne.

8.4.7.10 Załącznik 19 zawiera wymagania dotyczące struktury systemu SMS. Państwa transponują wymagania do swoich przepisów prawnych. Działanie dowolnego systemu lub procesu organizacji w praktyce zależy od sposobu wdrożenia wymagań. Istnieją dwa główne komponenty związane z równoważnością systemu SMS i konsekwencjami akceptacji SMS przez Państwa.

8.4.7.11 Pierwszy komponent to formalne aspekty wynikające z uznania lub akceptacji SMS. Niektóre Państwa rozwiązały tą kwestię poprzez zawarcie dwustronnych lub wielostronnych umów, które zawierają ustalenia dyplomatyczne, prawne i techniczne pomiędzy Państwami. W niektórych przypadkach akceptacja jest wzajemna, jednak nie we wszystkich okolicznościach.

8.4.7.12 Drugim komponentem jest równoważność techniczna. Równoważność techniczną można podzielić na pięć obszarów:

- a) *Wspólne wymagania.* Chociaż nie jest to wystarczające do ustanowienia równoważności, użycie wspólnego zestawu wymagań zapewnia strukturę i skuteczność ocen technicznych. Zostały one ustalone w różnych Załącznikach ICAO.
- b) *Oczekiwania dotyczące wdrożenia.* Każde Państwo określa konkretne oczekiwania dotyczące procesów, programów, metod i narzędzi dla innego organu w celu wykazania wdrożenia i działania systemu.
- c) *Metodologia akceptacji.* Metody, które są wykorzystywane przez Państwa do oceny stopnia zróżnicowania procesów i możliwości zarządzania pomiędzy Państwami. Zazwyczaj jest to funkcja krajowego systemu nadzoru nad bezpieczeństwem Państwa (CE-6, obowiązki licencjonowania, certyfikacji, upoważniania i zatwierdzania).
- d) *Pomiar wydajności.* Metodologia stosowana przez każde Państwo do pomiaru poziomu bezpieczeństwa certyfikowanej i zatwierdzonej organizacji ma na celu poprawę zrozumienia przez Państwo potencjału wydajności i statusu każdej organizacji.
- e) *Polityki i metody monitorowania.* Monitorowanie musi zapewniać informacje o stanie działania organizacji i ich systemów SMS. Jest to aspekt związany z obowiązkiem prowadzenia nadzoru przez

Państwo. Każde Państwo musi wypracować zrozumienie i zaufanie do metod stosowanych przez inny organ do nadzorowania systemów SMS. Umożliwia to akceptację lub uznanie systemów SMS.

8.4.7.13 System SMS podmiotów lotniczych musi zostać zaakceptowany przez właściwy organ Państwa. Oczekuje się, że podmioty lotnicze przeprowadzą analizę luk i opracują wykonalny plan wdrożenia (w tym akceptację przez Państwo jako planowanego zadania). Wdrożenie systemu SMS jest zazwyczaj prowadzone w trzech lub czterech etapach. Współpraca pomiędzy podmiotem i właściwym organem Państwa na wczesnym etapie powoduje, że proces opracowania i akceptacji przebiega sprawniej. W celu uzyskania informacji na temat wdrożenia systemu SMS, patrz Rozdział 9.

Akceptacja SPI i SPT

8.4.7.14 Wskaźniki SPI proponowane przez podmiot lotniczy są weryfikowane i akceptowane przez właściwy organ regulacyjny Państwa w ramach akceptacji systemu zarządzania bezpieczeństwem. Państwa mogą rozważyć planowanie akceptacji wskaźników SPI podmiotu na późniejszym etapie procesu wdrażania. Jest to szczególnie praktyczne dla podmiotów lotniczych przy wstępnej certyfikacji, ponieważ często nie mają one wystarczających danych, aby opracować sensowne wskaźniki. Regulator może być przekonany, że proponowane wskaźniki SPI są odpowiednie i stosowne do działalności lotniczej indywidualnego podmiotu. Niektóre SPI i SPT podmiotu lotniczego mogą mieć związek z SPI i SPT Państwa w zakresie pomiaru i monitorowania akceptowalnego poziomu bezpieczeństwa. Nie musi tak być w przypadku wszystkich SPI i SPT. Więcej informacji na temat pomiaru poziomu bezpieczeństwa znajduje się w Rozdziale 4.

8.4.7.15 Akceptacja SPT podmiotu lotniczego może mieć miejsce po zakończeniu okresu monitorowania SPI, w którym określana jest wydajność bazowa. Akceptacja może opierać się na celach ustalonych na poziomie krajowym, regionalnym lub globalnym. Osiągnięcie poziomu SPT przez Państwo będzie wymagało koordynacji działań łagodzących ryzyko bezpieczeństwa z podmiotem lotniczym.

Jeden system zarządzania bezpieczeństwem u wielu podmiotów lotniczych

8.4.7.16 Organizacje posiadające wiele certyfikatów podmiotu lotniczego mogą zdecydować o włączeniu ich wszystkich w zakres jednego systemu zarządzania bezpieczeństwem (SMS) w celu wykorzystania korzyści wynikających z SMS oraz lepszego rozwiązania aspektów związanych z interfejsami. Organ regulacyjny Państwa powinien rozważyć następujące kwestie podczas oceny systemu SMS tych organizacji macierzystych lub wdrożenia wymagań SMS w odniesieniu do podmiotów lotniczych, które są objęte zakresem szerszego systemu SMS:

- a) Należy upewnić się, że polityki i procesy monitorowania SMS są konsekwentnie stosowane w całym Państwie, w szczególności, gdy inspektorzy z różnych organizacji w ramach organu regulacyjnego są odpowiedzialni za nadzór i monitorowanie różnych podmiotów lotniczych:
 - 1) istnieją dowody na zaangażowanie kierownictwa w spójną interpretację przepisów i stosowanie nadzoru i monitorowania;
 - 2) wszystkim pracownikom zaangażowanym w nadzór i monitorowanie zapewniono standardowe szkolenie, najlepiej z udziałem przedstawicieli z różnych dziedzin;
 - 3) w przypadku występowania różnych organizacji prowadzących nadzór i monitorowanie, należy opracować i wdrożyć wspólne polityki, procedury i narzędzia audytowania;
 - 4) pomiędzy wyznaczonymi inspektorami przydzielonymi do każdego podmiotu lotniczego ma miejsce spójna i częsta komunikacja;
 - 5) wdrożono mechanizmy, które monitorują stopień standaryzacji działań nadzorczych i monitorujących. Należy rozwiązywać wszelkie zidentyfikowane problemy;

- 6) uznaje się, że działania podmiotu lotniczego mogą być objęte przez system SMS na poziomie korporacyjnym („macierzystym”). Może to dotyczyć działań, które wymagają posiadania systemu SMS oraz działań, które są poza zakresem zastosowania Załącznika 19.
- 7) organizacja macierzysta udokumentowała:
 - i) polityki i procedury dotyczące sposobu udostępniania danych bezpieczeństwa i informacji bezpieczeństwa, przekazywania komunikacji, podejmowania decyzji, oraz przydziału zasobów w różnych obszarach działalności oraz, w stosownych przypadkach, z różnymi organami regulacyjnymi;
 - ii) zakres obowiązków i odpowiedzialności związanych z systemem SMS; oraz
 - iii) strukturę organizacyjną i interfejsy pomiędzy różnymi systemami i działaniami w postaci opisu systemu.
- b) Należy mieć świadomość, że organizacje macierzyste posiadające wiele certyfikatów, spośród których część to certyfikaty od zagranicznych organów regulacyjnych, mogą zdecydować się na wdrożenie jednego systemu SMS w wielu podmiotach lotniczych.
 - 1) należy uznać, że zakres systemu SMS jest jasno przedstawiony w opisie systemu, który szczegółowo określa indywidualne działania. Podmiot lotniczy może wykazać kompatybilność pomiędzy procesami ich systemu SMS a korporacyjnym systemem SMS.
 - 2) należy mieć świadomość, że scenariusz ten może generować dodatkowe wyzwania w sytuacji gdy organizacja macierzysta posiada zarówno krajowe, jak i międzynarodowe zatwierdzenia, takie jak akceptacja systemu SMS przez różne organy regulacyjne. Należy zawrzeć porozumienie z innymi organami regulacyjnymi co do sposobu w jaki działania związane z nadzorem i monitorowaniem będą współdzielone, delegowane lub wykonywane oddzielnie (powielane), w sytuacji gdy procedury dotyczące akceptacji systemu SMS nie zostały jeszcze ustanowione.

Zintegrowane systemy zarządzania

8.4.7.17 Podczas oceny podmiotów lotniczych, którzy zintegrowali swoje systemy SMS z innymi systemami zarządzania, organ regulacyjny powinien rozważyć następujące kwestie:

- a) opracowanie projektu polityki, która określa zakres uprawnień (nie można być odpowiedzialnym za nadzór nad powiązаныmi systemami zarządzania); oraz
- b) zasoby niezbędne do oceny i monitorowania zintegrowanego systemu zarządzania (mogą one odnosić się do personelu posiadającego odpowiednią wiedzę oraz procesów, procedur i narzędzi).

8.4.7.18 Integracja systemu SMS z innymi systemami zarządzania niesie ze sobą korzyści dla podmiotu lotniczego. Integracja powinna zostać zakończona w sposób satysfakcjonujący władzę lotnictwa cywilnego, w taki sposób, aby mogła ona skutecznie „zobaczyć” i monitorować system. Wytyczne dla podmiotów lotniczych wdrażających system SMS jako część zintegrowanego systemu zarządzania znajdują się w Rozdziale 9.

8.4.8 Badanie wypadków

8.4.8.1 Komisja badania wypadków (AIA) musi być funkcjonalnie niezależna od jakiegokolwiek innej organizacji. Szczególne znaczenie ma niezależność od władzy lotnictwa cywilnego danego Państwa. Interesy władzy lotnictwa cywilnego mogą kolidować z zadaniami powierzonymi komisji badania wypadków. Uzasadnieniem dla niezależności tej funkcji od innych organizacji jest to, że związki przyczynowe wypadków mogą być powiązane

z czynnikami regulacyjnymi lub związanymi z SSP. Ponadto, taka niezależność wzmacnia wiarygodność komisji i pozwala uniknąć rzeczywistych lub postrzeganych konfliktów interesów.

8.4.8.2 Proces badania wypadków odgrywa kluczową rolę w SSP. Umożliwia on Państwu identyfikację czynników sprawczych i ewentualnych uchybień w systemie lotniczym, oraz generowanie niezbędnych środków zaradczych w celu zapobiegania ich ponownemu wystąpieniu. Działalność ta przyczynia się do ciągłego doskonalenia bezpieczeństwa lotniczego poprzez odkrywanie uchybień aktywnych i czynników sprawczych wypadków/incydentów oraz poprzez dostarczanie raportów na temat wszelkich doświadczeń zdobytych w wyniku analizy wydarzeń. Może to pomóc w wypracowaniu decyzji dotyczących działań naprawczych i odpowiedniej alokacji zasobów oraz może zidentyfikować konieczne ulepszenia systemu lotniczego. W celu uzyskania odpowiednich wytycznych i bardziej szczegółowych informacji, patrz Załącznik 13 ICAO.

8.4.8.3 Istnieje wiele zdarzeń związanych z bezpieczeństwem, które nie wymagają oficjalnego badania zgodnie z przepisami Załącznika 13. Zdarzenia te oraz zidentyfikowane zagrożenia mogą wskazywać na problemy systemowe. Problemy te mogą zostać ujawnione i usunięte w ramach badania bezpieczeństwa prowadzonego przez podmiot lotniczy. Informacje na temat badań bezpieczeństwa prowadzonych przez podmiot lotniczy, patrz Rozdział 9.

8.4.9 Identyfikacja zagrożeń i ocena ryzyka bezpieczeństwa

Ogólne wytyczne

8.4.9.1 Jedną z najważniejszych ról władz lotniczych jest identyfikacja zagrożeń i pojawiających się trendów w całym systemie lotniczym. Jest ona często realizowana poprzez analizę danych bezpieczeństwa zagregowanych z wielu źródeł. Poziom złożoności i zaawansowania procesu zarządzania ryzykiem bezpieczeństwa (SRM) będzie się różnić w zależności od wielkości, dojrzałości i złożoności systemu lotniczego Państwa. Ogólne wytyczne w zakresie procesu SRM znajdują się w Rozdziale 2.

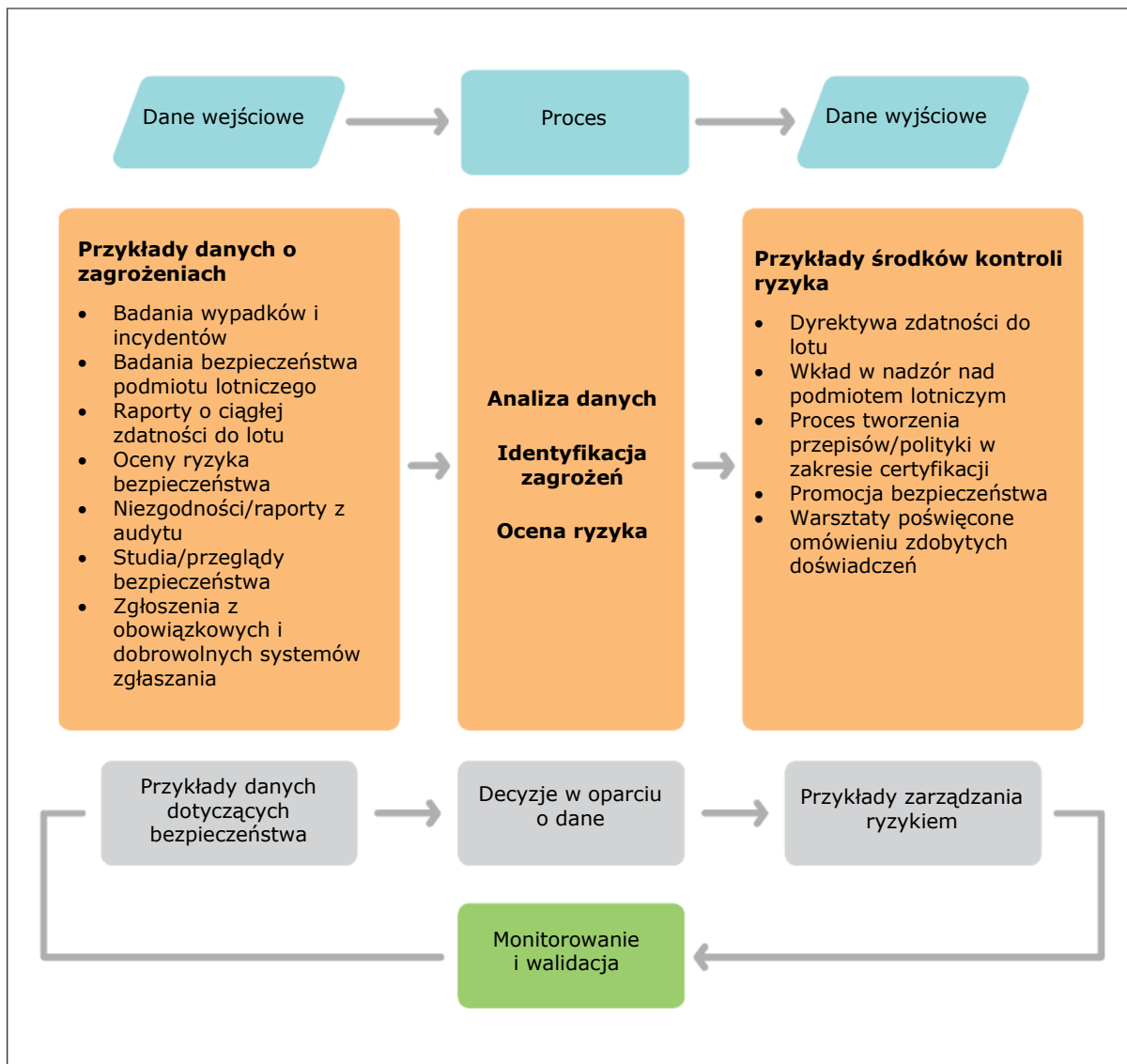
8.4.9.2 Zbieranie wewnętrznych i zewnętrznych danych bezpieczeństwa oraz informacji bezpieczeństwa jest niezbędne do uzyskania skutecznego SSP. Nieskomplikowane systemy lotnicze mogą generować ograniczone dane. W takim przypadku zbieranie i wymiana danych zewnętrznych powinny być priorytetem. Dane zewnętrzne są często dostępne z innych Państw w postaci np. raportów z badań, rocznych raportów bezpieczeństwa (w tym informacji i analiz dotyczących incydentów), ostrzeżeń dotyczących bezpieczeństwa, biuletynów bezpieczeństwa, studiów bezpieczeństwa, iSTARS, itp. Na poziomie regionalnym grupy ICAO (np. RASG, PIRG, itp.) mogą również stanowić dobre źródło informacji bezpieczeństwa. System zbierania i przetwarzania danych bezpieczeństwa (SDCPS) powinien obejmować procedury przekazywania raportów z badań wypadków i incydentów do ICAO, co ułatwi zbieranie i udostępnianie informacji bezpieczeństwa w skali światowej.

8.4.9.3 Głównym celem SRM jest identyfikacja i kontrola potencjalnych konsekwencji zagrożeń z wykorzystaniem dostępnych danych bezpieczeństwa. Zasady dotyczące SRM są takie same dla Państw i podmiotów lotniczych.

8.4.9.4 Podmioty lotnicze mają dostęp do własnych danych bezpieczeństwa. Państwa mają dostęp do danych bezpieczeństwa od wielu podmiotów lotniczych. W związku z tym wdrożenie przez Państwo wspólnych taksonomii służących klasyfikacji gromadzonych przez siebie danych bezpieczeństwa znacznie poprawi skuteczność procesu SRM. Pozwoli to również na bardziej efektywną analizę danych zebranych z wielu źródeł w różnych sektorach lotnictwa. Dane wejściowe i wyjściowe procesu analizy danych przedstawione zostały na Rysunku 8-2 poniżej.

8.4.9.5 Dane wejściowe mogą być otrzymywane z dowolnej części systemu lotniczego, w tym: z zakresu badań wypadków, badań bezpieczeństwa podmiotu lotniczego, raportów ciągłej zdatności do lotu, wyników ocen medycznych, ocen ryzyka bezpieczeństwa, wniosków i raportów z audytów oraz studiów i przeglądów bezpieczeństwa.

8.4.9.6 W razie konieczności stosuje się środki kontroli danych wyjściowych lub ryzyk bezpieczeństwa w celu wyeliminowania zagrożenia lub zmniejszenia poziomu ryzyka bezpieczeństwa do akceptowalnego poziomu. Kilka spośród wielu opcji łagodzenia dostępnych dla Państwa to dyrektywy dotyczące zdatości do lotu, zapewnienie wkładu w dopracowany system nadzoru i monitorowania podmiotów lotniczych, zmiany w certyfikacji, tworzenie przepisów lub polityka bezpieczeństwa, program promocji bezpieczeństwa, warsztaty poświęcone zdobytym doświadczeniom. Wybrane działanie będzie oczywiście zależało od dotkliwości i rodzaju problemu, którego dotyczy.



Rysunek 8-2. Program analizy w oparciu o dane

Identyfikacja zagrożeń

8.4.9.7 Identyfikacja zagrożeń opiera się na zbieraniu reprezentatywnych danych. Wskazane może być łączenie lub agregowanie danych z wielu sektorów w celu pełnego zrozumienia każdego zagrożenia. Proces przedstawiony na Rysunku 8-2 jest równie ważny dla reaktywnej lub proaktywnej identyfikacji zagrożeń. Analiza zagrożeń zidentyfikowanych podczas badania incydentu lub wypadku stanowi przykład metodologii reaktywnej. Metodologia proaktywna może obejmować zagrożenia zidentyfikowane podczas audytów lub inspekcji lub na podstawie obowiązkowych zgłoszeń. Może ona obejmować ostrzeżenie o wczesnych oznakach pogorszenia bezpieczeństwa na podstawie rutynowego monitorowania niezawodności systemu.

8.4.9.8 Zagrożenia występują na wszystkich poziomach systemu lotniczego Państwa. Wypadki lub incydenty występują, kiedy zagrożenia wchodzi w interakcje z pewnymi czynnikami uruchamiającymi. W rezultacie zagrożenia należy zidentyfikować, zanim doprowadzą do wypadków, incydentów lub innych zdarzeń związanych z bezpieczeństwem.

8.4.9.9 Zachęca się Państwa do wyznaczenia osoby lub zespołu do gromadzenia, agregowania i analizowania dostępnych danych. Analityk bezpieczeństwa powinien analizować dane w celu zidentyfikowania i udokumentowania potencjalnych zagrożeń, a także odpowiednich skutków lub konsekwencji. Poziom szczegółowości wymagany w procesie identyfikacji zagrożeń uzależniony jest od złożoności rozpatrywanego procesu.

8.4.9.10 Należy opracować systematyczny proces zapewniający skuteczną identyfikację zagrożeń. Powinien on uwzględniać następujące elementy:

- a) dostęp do źródeł danych niezbędnych do wsparcia zarządzania ryzykiem bezpieczeństwa w Państwie;
- b) zespół ds. analizy bezpieczeństwa z odpowiednimi umiejętnościami analitycznymi i doświadczeniem operacyjnym oraz szkoleniem i doświadczeniem z zakresu różnych technik analizy zagrożeń; oraz
- c) narzędzie (-a) do analizy zagrożeń, odpowiednie dla danych, które są zbierane (lub będą zbierane) oraz dla zakresu działalności lotniczej w Państwie.

Czynniki uruchamiające identyfikację zagrożeń

8.4.9.11 Istnieje wiele sytuacji, w których należy rozpocząć identyfikację zagrożeń. Niektóre z nich to:

- a) *Projekt systemu*: Identyfikacja zagrożeń rozpoczyna się przed rozpoczęciem operacji wraz ze szczegółowym opisem konkretnego systemu lotniczego i jego otoczenia. Zespół ds. analizy bezpieczeństwa identyfikuje różne potencjalne zagrożenia związane z systemem, jak również wpływ na inne systemy współpracujące.
- b) *Zmiana systemu*: Identyfikacja zagrożeń rozpoczyna się przed wprowadzeniem zmiany w systemie (operacyjnej lub organizacyjnej) i zawiera szczegółowy opis konkretnej zmiany w systemie lotniczym. Zespół ds. analizy bezpieczeństwa identyfikuje potencjalne zagrożenia związane z proponowaną zmianą, jak również wpływ na inne systemy współpracujące.
- c) *Na żądanie lub monitorowanie ciągle*: Identyfikacja zagrożeń dotyczy istniejących systemów będących w eksploatacji. Monitorowanie danych służy do wykrywania zmian w sytuacji zagrożenia. Na przykład pojawienie się zagrożenia może być częstsze lub bardziej dotkliwe niż się spodziewano, lub uzgodnione strategie łagodzenia są mniej skuteczne niż oczekiwano. Ciągłe monitorowanie i analiza mogą być ustalone za pomocą progów powiadamiania w oparciu o zestaw krytycznych elementów zainteresowania.

Ocena ryzyka bezpieczeństwa

8.4.9.12 Ogólne wytyczne w zakresie oceny ryzyka bezpieczeństwa znajdują się w Rozdziale 2. Należy zauważyć, że ryzyko bezpieczeństwa można obserwować i kontrolować w lotnictwie na poziomie sektora lub regionu.

8.4.9.13 Istnieje wiele różnych narzędzi analizy danych i wykorzystania różnych podejść do modelowania ryzyka bezpieczeństwa. Wybierając lub opracowując ocenę ryzyka bezpieczeństwa, Państwa powinny zapewnić, że proces działa dobrze w środowisku.

8.4.10 Zarządzanie ryzykami bezpieczeństwa

8.4.10.1 Wytyczne w zakresie rozwiązywania problemów związanych z bezpieczeństwem (CE-8) znajdują się w Doc 9734, Część A.

8.4.10.2 Zarządzanie ryzykiem bezpieczeństwa ma na celu zapewnienie kontroli ryzyk bezpieczeństwa i osiągnięcie akceptowalnego poziomu bezpieczeństwa (ALoSP). Właściwy organ Państwa opracowuje, dokumentuje i rekomenduje odpowiednie strategie łagodzenia lub kontroli ryzyka bezpieczeństwa. Przykłady obejmują: bezpośrednią interwencję w podmiocie lotniczym, wdrażanie dodatkowych polityk lub przepisów, wydawanie dyrektyw operacyjnych lub wpływanie na działania promocyjne związane z bezpieczeństwem.

8.4.10.3 Ocena każdego proponowanego środka kontroli ryzyka bezpieczeństwa powinna być przeprowadzona jako następny krok. Idealne propozycje w zakresie kontroli ryzyka bezpieczeństwa są opłacalne, łatwe do wykonania, szybko wdrażane, skuteczne i nie powodują niezamierzonych konsekwencji. Ponieważ większość sytuacji nie spełnia tych warunków, propozycje środków kontroli ryzyka bezpieczeństwa powinny być oceniane i wybierane w oparciu o równoważenie atrybutów skuteczności, kosztów, terminowości wdrożenia i złożoności. Kiedy środki kontroli ryzyka bezpieczeństwa zostały wybrane i wdrożone, należy je monitorować i walidować w celu zapewnienia, że zamierzone cele zostały osiągnięte.

8.4.10.4 Wiele środków kontroli ryzyka bezpieczeństwa wymaga działania ze strony podmiotów lotniczych. Państwa powinny kierować podmiotem (-ami) do skutecznego wdrożenia. Państwa mogą potrzebować monitorować skuteczność środków kontroli ryzyka bezpieczeństwa i ich wpływ na poziom bezpieczeństwa podmiotów lotniczych, łącznie na poziom bezpieczeństwa Państw. Podejścia do łagodzenia ryzyka bezpieczeństwa przedstawione zostały w Rozdziale 2.

8.5. KOMPONENT NR 3: ZAPEWNIENIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

8.5.1 Działania w zakresie zapewnienia bezpieczeństwa przez Państwo mają na celu zapewnienie Państwa, że jego funkcje osiągają zamierzone cele ogólne i cele szczegółowe w zakresie bezpieczeństwa. Podmioty lotnicze są zobowiązane do wdrożenia procesu zapewnienia bezpieczeństwa w ramach systemu zarządzania bezpieczeństwem. Możliwość zapewnienia SMS zapewnia każdy podmiot lotniczy, że jego procesy bezpieczeństwa funkcjonują skutecznie, i że jest on na dobrej drodze do osiągnięcia swoich celów ogólnych w zakresie bezpieczeństwa. Podobnie, działania w zakresie zapewnienia bezpieczeństwa przez Państwo, w ramach ich krajowego programu bezpieczeństwa, zapewniają Państwo, że jego procesy bezpieczeństwa funkcjonują skutecznie, a Państwo jest na dobrej drodze do osiągnięcia swoich celów ogólnych w zakresie bezpieczeństwa poprzez zbiorowy wysiłek branży lotniczej Państwa.

8.5.2 Działania związane z nadzorem oraz mechanizmy gromadzenia, analizy, udostępniania i wymiany danych/informacji bezpieczeństwa zapewniają, że środki kontroli ryzyka bezpieczeństwa są odpowiednio zintegrowane z systemem SMS podmiotu lotniczego. Daje to pewność, że system działa zgodnie z założeniami, a środki kontroli odnoszą zamierzony efekt w zakresie zarządzania ryzykiem bezpieczeństwa. Państwa mogą zbierać dane/informacje bezpieczeństwa lotniczego z wielu źródeł, w tym za pomocą procesów nadzoru i programów zgłaszania zdarzeń dotyczących bezpieczeństwa. Dane powinny być analizowane na różnych poziomach, a wnioski wyciągane z analizy powinny być wykorzystywane jako podstawa do podejmowania świadomych decyzji dotyczących bezpieczeństwa w odniesieniu do działań w zakresie nadzoru i bezpieczeństwa systemu lotniczego Państwa.

8.5.3 Obowiązek prowadzenia nadzoru

8.5.3.1 Wytyczne w zakresie obowiązków prowadzenia nadzoru (CE-7) związanych z monitorowaniem zgodności znajdują się w Doc 9734, Część A.

Ustalenie priorytetów w zakresie działań nadzorczych

8.5.3.2 Podejście do nadzoru w oparciu o ryzyko bezpieczeństwa (SRBS) umożliwia ustalanie priorytetów i przydzielanie zasobów zarządzania bezpieczeństwem Państwa proporcjonalnie do profilu ryzyka bezpieczeństwa każdego sektora lub indywidualnego podmiotu lotniczego. Państwa zdobywają doświadczenie i wiedzę na temat każdego podmiotu lotniczego poprzez monitorowanie stale rozwijającej się dojrzałości ich procesu zapewniania bezpieczeństwa, a w szczególności ich procesu zarządzania poziomem bezpieczeństwa. Z biegiem czasu Państwo będzie budować obraz zdolności podmiotu w zakresie bezpieczeństwa, ze szczególnym uwzględnieniem zarządzania ryzykiem bezpieczeństwa. Państwo może zdecydować się na zmianę zakresu i/lub częstotliwości nadzoru w miarę rozwoju zaufania i pozyskiwania dowodów na możliwości podmiotu w zakresie bezpieczeństwa.

8.5.3.3 Nadzór w oparciu o ryzyko bezpieczeństwa (SRBS) jest najbardziej odpowiedni dla organizacji z dojrzałym systemem SMS. SRBS może mieć również zastosowanie do organizacji, w których system SMS nie został jeszcze wdrożony. Podstawą skutecznego SRBS są wystarczająco wiarygodne i znaczące dane. Bez wiarygodnych i znaczących danych trudno jest obronić zmiany zakresu lub częstotliwości nadzoru.

8.5.3.4 Państwa powinny rozwijać lub wzmacniać swoje możliwości zarządzania danymi w celu zapewnienia, że są w posiadaniu wiarygodnych i wyczerpujących danych, na których można oprzeć swoje decyzje (w oparciu o dane). Analizy ryzyka dla poszczególnych sektorów mogą również pozwolić Państwu na ocenę wspólnych ryzyk bezpieczeństwa, które wpływają na wiele podmiotów lotniczych o podobnych rodzajach operacji (na przykład linie lotnicze wykonujące operacje krótkiego zasięgu). Ułatwia to stworzenie rankingu ryzyka bezpieczeństwa wśród podmiotów lotniczych w określonym sektorze lotnictwa lub pomiędzy sektorami, oraz wspiera alokację zasobów w zakresie nadzoru do sektorów lub działań o największym wpływie na bezpieczeństwo.

8.5.3.5 Analizy na poziomie sektora zapewniają Państwu obraz systemu lotniczego w kontekście sposobu, w jaki poszczególne części przyczyniają się do działania całości. Umożliwiają one Państwu określenie sektorów, które skorzystają na wyższym poziomie wsparcia lub interwencji, a które są najlepszymi kandydatami do podejścia opartego na współpracy. Daje to Państwu pewność, że regulacje w całym systemie lotniczym są współmierne i ukierunkowane na obszary o największych potrzebach. Łatwiej jest zidentyfikować obszary, w których konieczne są zmiany w określonych przepisach w celu osiągnięcia maksymalnej skuteczności regulacyjnej przy minimalnej ingerencji.

8.5.3.6 SRBS ma swoją cenę. Wymaga on ciągłej interakcji pomiędzy Państwem a społecznością lotniczą poza kontrolami i inspekcjami zgodności. Podejście SRBS wykorzystuje profil ryzyka podmiotu lotniczego w celu dostosowania swoich działań w zakresie nadzoru. Wyniki wewnętrznych przeglądów, analiz i decyzji w ramach systemu podmiotu stają się ukierunkowanym planem działania określającym kluczowe ryzyka bezpieczeństwa oraz środki łagodzenia, które skutecznie je rozwiązują. Analiza przeprowadzona zarówno przez Państwo, jak i podmiot lotniczy określa obszary priorytetowe w zakresie bezpieczeństwa i przedstawia najskuteczniejsze sposoby ich rozwiązania.

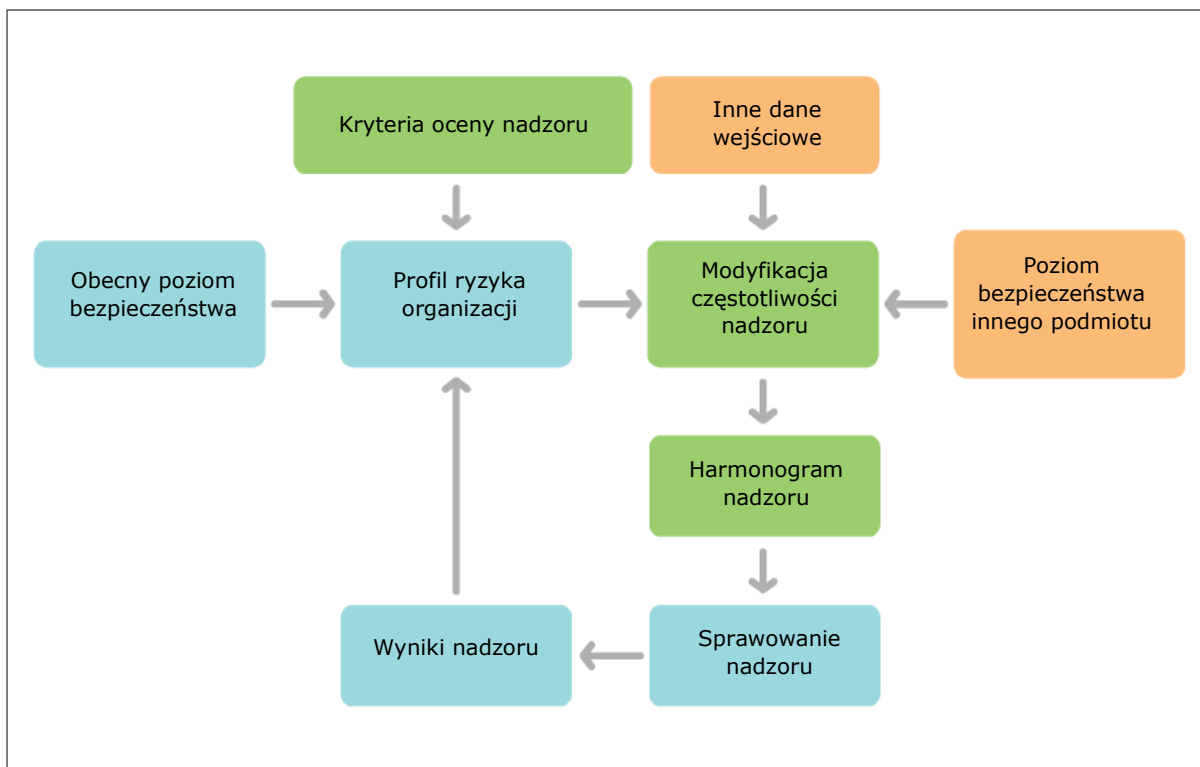
8.5.3.7 Co ważne, nadzór w oparciu o ryzyko bezpieczeństwa nie musi koniecznie ograniczać zakresu prowadzonego nadzoru lub zasobów. Jakość nadzoru i jakość interakcji pomiędzy organem regulacyjnym a podmiotem lotniczym ulegną jednak znacznej poprawie.

Profile ryzyka organizacji w odniesieniu do podmiotu lotniczego

8.5.3.8 Państwa mogą chcieć opracować profile ryzyka organizacji, które są spójne w każdym sektorze lotnictwa w celu wsparcia procesu modyfikacji zakresu i częstotliwości prowadzenia swoich działań nadzorczych. Takie narzędzia powinny być ukierunkowane na pozyskiwanie i agregowanie informacji, które powinny być dostępne dla podmiotów lotniczych i mogą dotyczyć następujących czynników:

- a) kondycja finansowa organizacji;
- b) czas prowadzenia działalności;
- c) poziom fluktuacji kluczowego personelu, np. dyrektora odpowiedzialnego i kierownika ds. bezpieczeństwa;
- d) kompetencje i wyniki dyrektora odpowiedzialnego;
- e) kompetencje i wyniki kierownika ds. bezpieczeństwa; (więcej informacji na temat kompetencji dyrektora odpowiedzialnego lub kierownika ds. bezpieczeństwa, patrz Rozdział 9)
- f) wyniki poprzednich audytów;
- g) terminowe i skuteczne usuwanie wcześniejszych niezgodności;
- h) pomiary względnego poziomu działalności (narażenie na ryzyko bezpieczeństwa);
- i) wskaźniki względnego zakresu i złożoności wykonywanych działań;
- j) dojrzałość procesu identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa; oraz
- k) pomiary poziomu bezpieczeństwa na podstawie analizy danych bezpieczeństwa i monitorowania wyników przez Państwo.

8.5.3.9 Przykład procesu, który może być użyty do modyfikacji zakresu lub częstotliwości prowadzenia działań nadzorczych nad podmiotem lotniczym, przedstawiony został na Rysunku 8-3.



Rysunek 8-3. Koncepcja nadzoru w oparciu o ryzyko bezpieczeństwa

8.5.4 Monitorowanie poziomu bezpieczeństwa podmiotu lotniczego

Państwo powinno dokonywać okresowych przeglądów wskaźników SPI i poziomu SPT każdego podmiotu lotniczego. Przegląd powinien uwzględniać działanie i skuteczność każdego SPI i SPT. Przegląd może wykazać potrzebę wprowadzenia zmian w celu wsparcia ciągłego doskonalenia bezpieczeństwa.

8.5.5 Poziom bezpieczeństwa Państwa

8.5.5.1 Ogólne informacje na temat zarządzania poziomem bezpieczeństwa znajdują się w Rozdziale 4.

Akceptowalny poziom bezpieczeństwa

8.5.5.2 Państwa muszą ustanowić akceptowalny poziom bezpieczeństwa (ALoSP), który należy osiągnąć poprzez krajowy program bezpieczeństwa (SSP). Można to osiągnąć poprzez:

- a) wdrożenie i utrzymanie SSP; oraz
- b) wdrożenie i utrzymanie SPI i SPT, które pokazują, że bezpieczeństwo jest skutecznie zarządzane.

8.5.5.3 ALoSP wyraża poziom bezpieczeństwa, których Państwo oczekuje od swojego systemu lotniczego, w tym cele, które każdy sektor musi osiągnąć i utrzymać w odniesieniu do bezpieczeństwa, a także środki mające na celu określenie skuteczności działań i funkcji mających wpływ na bezpieczeństwo. ALoSP stanowi zatem odzwierciedlenie tego, co Państwo uznaje za ważne, oraz jest on uzgodniony przez zainteresowane strony na poziomie Państwa. ALoSP nie powinien być opracowywany jako oddzielne zagadnienie. Powinien być raczej zdefiniowany z uwzględnieniem wytycznych strategicznych wyższego szczebla (na podstawie GASP, planów regionalnych, itp.) oraz celów w zakresie bezpieczeństwa ustanowionych w SSP.

Ustanowienie akceptowalnego poziomu bezpieczeństwa (ALoSP)

8.5.5.4 Odpowiedzialność za ustanowienie ALoSP spoczywa na władzach lotniczych Państwa i będzie on wyrażony poprzez zestaw wskaźników SPI w odniesieniu do Państwa, sektorów i podmiotów lotniczych podlegających ich jurysdykcji. Celem jest utrzymanie lub ciągle podnoszenie poziomu bezpieczeństwa w ramach procesu pomiaru, o którym mowa w Rozdziale 4. Pozwala to Państwu zrozumieć sposób działania w odniesieniu do bezpieczeństwa oraz pozwala wpływać na sytuację kiedy zajdzie taka potrzeba. Akceptacja wskaźników SPI i poziomów SPT podmiotów lotniczych jest częścią tego procesu.

8.5.5.5 ALoSP stanowi porozumienie pomiędzy wszystkimi władzami lotniczymi Państwa w sprawie oczekiwanego poziomu bezpieczeństwa, który powinien zapewnić system lotniczy, oraz pokazuje wewnętrznym i zewnętrznym zainteresowanym stronom, w jaki sposób Państwo zarządza bezpieczeństwem lotniczym. Dotyczy to, między innymi, oczekiwań w zakresie poziomu bezpieczeństwa dla każdego sektora i podmiotu lotniczego, które podlegają władzy lotniczej Państwa. Ustanowienie ALoSP nie zastępuje ani nie znosi obowiązku Państwa dotyczącego przestrzegania Konwencji o międzynarodowym lotnictwie cywilnym, w tym wdrożenia wszystkich mających zastosowanie norm i zalecanych metod postępowania.

8.5.5.6 Rysunek 8-4 przedstawia koncepcję ALoSP w oparciu o SPI i SPT. Dalsze informacje na temat celów bezpieczeństwa, SPI i SPT znajdują się w Rozdziale 4 i w kolejnych punktach.

Wskaźniki poziomu bezpieczeństwa (SPI) i cele poziomów bezpieczeństwa (SPT)

8.5.5.7 SPI powinny odzwierciedlać konkretne środowisko operacyjne i służyć do podkreślenia warunków, które mogą być wykorzystane do określenia sposobu, w jaki kontrolowane są ryzyka bezpieczeństwa. Strategia monitorowania i pomiaru powinna zawierać zestaw wskaźników SPI obejmujących wszystkie obszary systemu lotniczego, za które odpowiedzialne jest Państwo. Powinna ona odzwierciedlać zarówno wyniki (np. wypadki, incydenty, naruszenia przepisów), jak i funkcje i działania (operacje, w których wprowadzono środki łagodzenia ryzyka bezpieczeństwa zgodnie z oczekiwaniami). Połączenie to pozwala na ocenę poziomu bezpieczeństwa nie tylko na podstawie tego, co nie działa (tj. wyniki), ale również z uwzględnieniem tego, co działa (tj. działania, w których środki łagodzenia ryzyka bezpieczeństwa przyniosły oczekiwane rezultaty). W praktyce podejście to obejmuje uwzględnienie SPI odzwierciedlające dwa odrębne rodzaje ryzyk bezpieczeństwa:

- a) **Ryzyko operacyjne** (przedstawione po lewej stronie diagramu) koncentruje się na warunkach, które mogą prowadzić do niepożądanego wyniku. Są to warunki związane z wypadkami, incydentami, uchybieniami i wadami. Ryzyko operacyjne jest zasadniczo produktem ubocznym świadczenia usług. Z tego powodu wskaźniki SPI koncentrujące się na ryzyku operacyjnym będą w większości powiązane – pośrednio – z systemem zarządzania bezpieczeństwem podmiotów lotniczych. Chociaż Rysunek 8-4 przedstawia trzy ryzyka operacyjne, rzeczywista liczba powinna opierać się na sytuacji w danym Państwie.

Te wskaźniki SPI odzwierciedlają głównie problemy związane z bezpieczeństwem operacyjnym zidentyfikowane w procesie SRM podmiotów lotniczych. Proces SRM Państwa może być również wykorzystany jako wkład odzwierciedlający problemy związane z bezpieczeństwem operacyjnym w całym systemie lotnictwa w wyniku agregacji wskaźników SPI dotyczących ryzyka operacyjnego. Często pojawia się relacja typu jeden-do-wielu pomiędzy problemem związanym z bezpieczeństwem operacyjnym a powiązаныmi wskaźnikami SPI. Polega to na tym, że jeden problem związany z bezpieczeństwem operacyjnym może być wskazany przez kilka wskaźników SPI.

- b) **Ryzyko związane z wdrożeniem procesów** (przedstawione po prawej stronie diagramu) koncentruje się na środkach i zasobach niezbędnych do zarządzania ryzykiem operacyjnym. Zarządzanie ryzykiem bezpieczeństwa z perspektywy wdrożenia procesu rozpoczyna się od oceny statusu wdrożenia SARP ICAO (krajowe przepisy i regulacje związane z bezpieczeństwem), wdrożenia procesów SMS w branży oraz wdrożenia SSP na poziomie Państwa (co obejmuje skuteczny nadzór

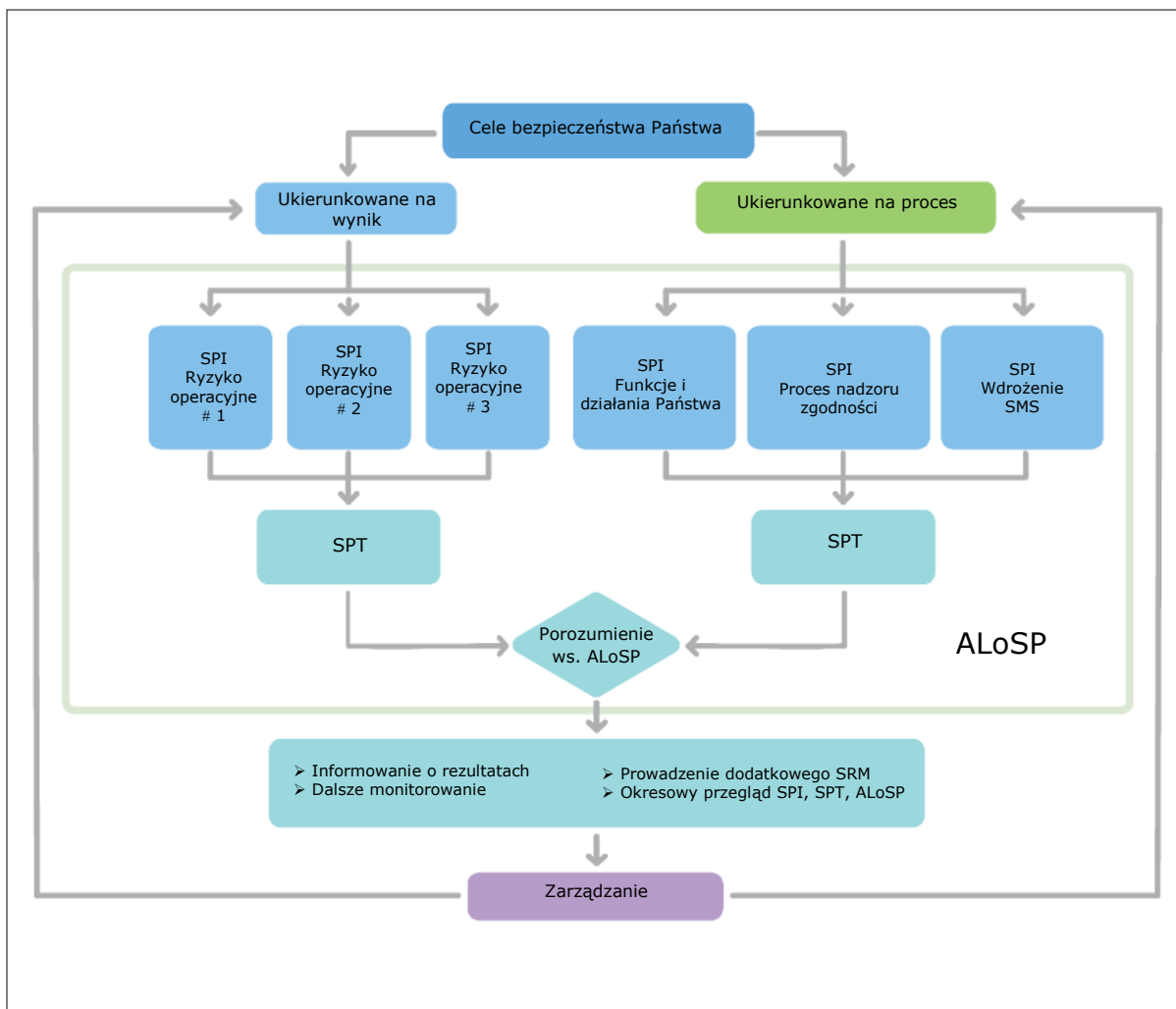
i monitorowanie branży). Jeżeli konieczne są ulepszenia któregokolwiek z powyższych obszarów, działania mające na celu ich osiągnięcie powinny zostać zaplanowane, wdrożone i monitorowane, oraz należy przeznaczyć odpowiednie zasoby na realizację tych działań. Następnie opracowuje się SPI, które umożliwiają śledzenie planowania, wdrażania i/lub skuteczności wprowadzonych zmian.

Wskaźniki SPI koncentrujące się na „ryzyku związanym z wdrożeniem procesów” zapewniają Państwu alternatywne środki inne aniżeli ścisłe przestrzeganie, aby monitorować adekwatność procedur organizacji w zakresie SMS oraz wdrożenia procesów SRM/zapewnienia bezpieczeństwa przez podmioty lotnicze. Te wskaźniki SPI można również ustanowić poprzez odniesienie do potrzebnych ulepszeń, jak pokazują analizy USOAP i działania ciągłego doskonalenia SSP. Wyniki audytów USOAP, agregacja ocen SMS i ciągłe doskonalenie SSP określają potencjalne obszary do poprawy. Powinny one być traktowane priorytetowo zgodnie z największą możliwą do osiągnięcia korzyścią. Przyczyni się to do poprawy poziomu bezpieczeństwa systemu lotniczego Państwa. Te wskaźniki SPI powinny różnić się od SPI dotyczących ryzyka operacyjnego.

8.5.5.8 Wskaźniki SPI zarówno dla ryzyk operacyjnych jak i ryzyk związanych z wdrożeniem procesów stają się kluczowym elementem procesu zapewnienia bezpieczeństwa Państwa. Agregacja SPI dotyczących ryzyk operacyjnych oraz SPI dotyczących ryzyk związanych z wdrożeniem procesów poszerza źródło informacji zwrotnych służących do ustanowienia akceptowalnego poziomu bezpieczeństwa Państwa.

Okresowy przegląd wskaźników bezpieczeństwa

8.5.5.9 Po ustanowieniu wskaźników SPI na poziomie Państwa, konieczne jest prowadzenie okresowych przeglądów. Początkowo identyfikacja najważniejszych ryzyk bezpieczeństwa polega na działaniu wspomaganym przez analizę na podstawie danych historycznych. System lotniczy jest jednak dynamiczny i ciągle się zmienia. Mogą pojawić się nowe problemy związane z bezpieczeństwem, procesy w obrębie Państwa mogą ulec zmianie, itp. Okresowy przegląd problemów i procesów związanych z bezpieczeństwem operacyjnym stanowi wsparcie dla aktualizacji i doskonalenia celów w zakresie bezpieczeństwa, a w konsekwencji SPI i SPT.



Rysunek 8-4. Akceptowalny poziom bezpieczeństwa (ALoSP)

Okresowy przegląd akceptowalnego poziomu bezpieczeństwa

8.5.5.10 Kierownictwo wyższego szczebla odpowiedzialne za pierwotne porozumienie w sprawie ALoSP powinno określić ciągłą stosowność ALoSP. Okresowy przegląd ALoSP powinien koncentrować się na:

- identyfikacji krytycznych problemów związanych z bezpieczeństwem w sektorach lotniczych, zapewniając włączenie wskaźników SPI, które umożliwiają zarządzanie poziomem bezpieczeństwa w tych obszarach;
- identyfikacji SPT, które określają poziom bezpieczeństwa, który ma być utrzymany, lub pożądaną poprawę do osiągnięcia w odniesieniu do odpowiednich SPI w każdym sektorze, w celu poprawy zarządzania poziomem bezpieczeństwa w całym systemie lotniczym Państwa;
- identyfikacji czynników uruchamiających (jeżeli dotyczy), w sytuacji gdy SPI osiągnie punkt, który wymaga pewnych działań; oraz
- przeglądzie SPI w celu określenia, czy modyfikacje lub dodatki do istniejących SPI, SPT i czynników uruchamiających (jeżeli dotyczy) są potrzebne do osiągnięcia uzgodnionego ALoSP.

8.5.5.11 Efektem okresowego przeglądu najważniejszych ryzyk jest lepsze zrozumienie charakteru każdego problemu związanego z bezpieczeństwem operacyjnym w sposób tak szczegółowy, jak pozwalają na to dane.

Państwo powinno uwzględnić swoje zagrożenia i ich potencjalne konsekwencje na wszystkich poziomach systemu lotniczego. Należy również analizować, w jaki sposób procesy realizowane przez Państwo (licencjonowanie, certyfikacja, upoważnianie, zatwierdzanie, nadzór, itp.) przyczyniają się do zarządzania ryzykiem bezpieczeństwa. Każde ryzyko operacyjne podlega ocenie w celu określenia wymaganych środków łagodzenia ryzyka bezpieczeństwa. Działania te są monitorowane poprzez SPI, które mierzą ich skuteczność.

8.5.5.12 Poprawa poziomu bezpieczeństwa w zakresie ryzyka operacyjnego jest zazwyczaj reaktywna, podczas gdy poprawa procesów zarządzania ryzykiem bezpieczeństwa ma charakter proaktywny. Ulepszanie procesów Państwa, które lepiej wspierają zarządzanie ryzykiem bezpieczeństwa, umożliwia identyfikację i kontrolę zagrożeń, zanim przekształcą się one w negatywne skutki.

Osiągnięcie akceptowalnego poziomu bezpieczeństwa

8.5.5.13 Poziom bezpieczeństwa Państwa, wraz z SPI i SPT, świadczą o osiągniętym dopuszczalnym poziomie bezpieczeństwa. Jeżeli którykolwiek SPT nie zostanie spełniony, konieczne może być przeprowadzenie oceny, aby lepiej zrozumieć przyczynę i określić działania, które należy podjąć. Może tak się zdarzyć ponieważ:

- a) poziomy docelowy nie były osiągalne lub realistyczne;
- b) działania podjęte dla osiągnięcia poziomu docelowego nie były właściwe lub odbiegały od pierwotnej intencji (dryf praktyczny);
- c) zmiany w priorytetach związanych z ryzykiem bezpieczeństwa spowodowały, że zasoby przestały spełniać poziom docelowy; lub
- d) pojawiły się nowe ryzyka, które nie były brane pod uwagę przy ustalaniu poziomów docelowych.

8.5.5.14 W przypadku poziomów docelowych, które nie zostały spełnione, konieczne będzie zrozumienie przyczyn, oraz podjęcie decyzji przez kierownictwo czy poprawa bezpieczeństwa jest wystarczająca, nawet jeżeli poziom docelowy nie został osiągnięty, oraz jakie dalsze działania są potrzebne. Może to wymagać dodatkowej analizy, która mogłaby zidentyfikować niektóre czynniki ryzyka, które nie zostały uwzględnione, lub niektóre istniejące środki łagodzenia ryzyka, które nie są skuteczne.

8.5.6 Zarządzanie zmianą z perspektywy Państwa

8.5.6.1 Załącznik 19 nie wymaga w sposób jednoznaczny ustanowienia przez Państwo formalnych działań mających na celu zarządzania zmianą w ramach SSP. Jednak zmiany są wszechobecne we współczesnym systemie lotniczym. Po wprowadzeniu zmian w systemie, ustalony obraz ryzyka bezpieczeństwa w odniesieniu do systemu ulegnie zmianie. Zmiany mogą wprowadzać zagrożenia, które mogą mieć wpływ na skuteczność istniejących mechanizmów obronnych. Może to powodować pojawienie się nowego ryzyka lub zmiany w istniejących ryzykach bezpieczeństwa. Państwa powinny ocenić wpływ zmian w swoich systemach lotniczych i zarządzać nimi.

8.5.6.2 W ramach SSP należy opracować procedury oceny wpływu zmian na poziomie Państwa. Procedury powinny pozwalać Państwu na proaktywne określanie wpływu zmian w systemie lotniczym zanim zostaną one wdrożone, oraz na planowanie i wprowadzanie proponowanych zmian w uporządkowany sposób.

8.5.6.3 Na etapie planowania zmian, Państwo powinno przeanalizować wpływ zmiany na istniejący system oraz, korzystając z istniejącego procesu SRM, przeanalizować, ocenić i w razie potrzeby złagodzić wszelkie nowe lub zmienione ryzyka bezpieczeństwa. W zmienionym systemie lub kontekście operacyjnym nie powinna mieć miejsca żadna operacja, dopóki nie zostaną ocenione wszystkie ryzyka bezpieczeństwa.

8.5.6.4 Państwo będzie musiało zmierzyć się z dwoma rodzajami zmian w ramach SSP: zmiana organizacyjna (na przykład realokacja obowiązków lub restrukturyzacja w ramach władz lotniczych Państwa) i

zmiana operacyjna (na przykład zmiana wykorzystania przestrzeni powietrznej). Zarządzanie zmianą w ramach SSP powinno koncentrować się na tych zmianach, które mogą mieć znaczący wpływ na zdolność Państwa do wypełniania zobowiązań prawnych (zmiana procesu) i na możliwości zarządzania bezpieczeństwem przez Państwo. Może to obejmować połączenie zmian procesowych i operacyjnych.

8.5.6.5 Przykłady zmian, które mogą mieć znaczący wpływ na ryzyka bezpieczeństwa, obejmują między innymi:

- a) reorganizację władz lotniczych Państwa (w tym zmniejszenie zatrudnienia);
- b) zmiany w procesach SSP, w tym zmiany metodologii, np. SRBS, SRM i procesów zapewniania bezpieczeństwa;
- c) zmiany w otoczeniu prawnym, np. zmiany w istniejących politykach bezpieczeństwa, programach i przepisach;
- d) zmiany w środowisku operacyjnym, np. wprowadzenie nowych technologii, zmiany w infrastrukturze, wyposażeniu i usługach;
- e) szybko zmieniająca się branża (rozwój, kurczenie się, przekształcanie) i potencjalny wpływ na nadzór i monitorowanie działania przez Państwo.

8.5.6.6 Informowanie o zmianach ma zasadnicze znaczenie dla skuteczności zarządzania zmianą. Niezbędne jest, aby personel i podmioty lotnicze, dotknięci zmianą, byli jej świadomi, oraz znali harmonogram i skutki jej wprowadzenia.

8.6. KOMPONENT NR 4: PROMOWANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO

8.6.1 Z punktu widzenia Państwa, potrzeba wdrożenia wewnętrznych i zewnętrznych działań na rzecz promocji bezpieczeństwa została ustanowiona w Załączniku 19 jako jeden z elementów odpowiedzialności Państw za zarządzanie bezpieczeństwem. Wewnętrznie, władze lotnictwa cywilnego i inne władze lotnicze zaangażowane w SSP powinny ustanowić mechanizmy zapewniające pracownikom odpowiednie informacje bezpieczeństwa w celu wsparcia rozwoju kultury, która sprzyja skutecznemu i wydajnemu SSP. Informowanie o polityce bezpieczeństwa, planach bezpieczeństwa, a także innej ważnej dokumentacji związanej z SSP może również zwiększyć świadomość i współpracę pomiędzy pracownikami w taki sposób, aby procesy zarządzania bezpieczeństwem wprowadzone przez Państwa były skuteczne.

8.6.2 Poprawa poziomu bezpieczeństwa w danym Państwie lub określonym sektorze lotniczym jest w dużym stopniu uzależniona od kultury bezpieczeństwa. Działania związane z zarządzaniem bezpieczeństwem wydają się być bardziej skuteczne, kiedy organizacja ma pozytywną kulturę bezpieczeństwa. Przy wyraźnym wsparciu kierownictwa wyższego i średniego szczebla, pracownicy na pierwszej linii mają poczucie współodpowiedzialności za osiągnięcie celów w zakresie bezpieczeństwa.

8.6.3 Pośród działań na rzecz poprawy kultury bezpieczeństwa w systemie lotniczym, potrzeba komunikacja wyróżnia się pod względem znaczenia, jakie odgrywa. Poprzez nieustanne przekazywanie swoich priorytetów, najlepszych praktyk, wyróżniających ryzyk w danej operacji, Państwo może wspierać pozytywną kulturę bezpieczeństwa i zwiększać do maksimum potencjał osiągnięcia swoich celów w zakresie bezpieczeństwa, czy to wśród specjalistów władz lotnictwa cywilnego, czy też podmiotów lotniczych. Więcej informacji na temat kultury bezpieczeństwa znajduje się w Rozdziale 3.

8.6.4 Kiedy pracownicy rozumieją swoje obowiązki w zakresie bezpieczeństwa, oczekuje się, że będą aktywnie poszukiwać środków i informacji, które mogą zostać wykorzystane do skutecznego wypełniania obowiązków w

zakresie bezpieczeństwa lotniczego. Jest to szansa na to, aby promocja bezpieczeństwa odgrywała kluczową rolę w zarządzaniu bezpieczeństwem. Ustanowienie zewnętrznych kanałów komunikacji z podmiotami lotniczymi powinno umożliwić udostępnianie zdobytych doświadczeń, najlepszych praktyk, wskaźników SPI oraz informacji na temat konkretnych ryzyk bezpieczeństwa. Powinno to wspierać wdrażanie praktyk w zakresie zarządzania bezpieczeństwem wśród podmiotów lotniczych, wspierając rozwój pozytywnej kultury bezpieczeństwa wśród organizacji partnerskich. Ponadto ustanowienie rutynowych działań komunikacyjnych z podmiotami lotniczymi może zwiększyć ogólną świadomość problemów związanych z bezpieczeństwem lotniczym i zachęcić do dalszej współpracy w identyfikowaniu inicjatyw na rzecz poprawy bezpieczeństwa.

8.6.5 Ponieważ Państwa podejmują decyzje lub działania mające na celu poprawę bezpieczeństwa lotniczego (np. ustanawianie przepisów lub wprowadzanie zmian w metodach sprawowania nadzoru), ważne jest również, aby Państwa komunikowały się zarówno wewnątrz, jak i zewnątrz. Może to wzmocnić postrzeganie przez społeczność lotniczą ich zaangażowania. To z kolei może przyczynić się do osiągnięcia celów w zakresie bezpieczeństwa Państwa.

8.6.6 Dostępnych jest wiele zasobów i narzędzi służących wsparciu Państwa w ustanawianiu działań promujących bezpieczeństwo. Jednym ze sposobów organizacji wielu działań promocyjnych jest ustanowienie przez Państwo planu komunikacji. Taki plan mógłby obejmować, co najmniej, mapowanie zainteresowanych członków społeczności lotniczej, wiadomości i informacje przekazywane każdej z grup tej społeczności oraz środki, za pomocą których informacje te będą przekazywane. Plan komunikacji może również pełnić rolę mapy drogowej wspierającej władzę lotnictwa cywilnego w skutecznym rozwijaniu możliwości i kanałów komunikacji z odbiorcami wewnętrznymi i zewnętrznymi. Może on mieć zasadnicze znaczenie dla Państw budujących kulturę bezpieczeństwa, a także dla zapewnienia niezbędnych danych i narzędzi wymaganych przez skuteczne zarządzanie bezpieczeństwem, zarówno z perspektywy Państw, jak i podmiotów prowadzących działalność w lotnictwie cywilnym.

8.6.7 Niektóre informacje mogą być przekazywane za pośrednictwem mniej formalnych biuletynów i postów z wykorzystaniem mediów społecznościowych, podczas gdy inne lepiej jest przekazywać podczas specjalnych spotkań lub seminariów. Rolą Państwa jest wdrożenie odpowiednich kanałów promocji bezpieczeństwa oraz mediów, które ich zdaniem pozwolą osiągnąć najlepsze wyniki w rozwijaniu pozytywnej kultury bezpieczeństwa i ostatecznie osiągnąć skuteczny SSP oraz bezpieczniejszy system lotnictwa cywilnego w Państwie.

8.6.8 Komunikacja wewnętrzna i rozpowszechnianie informacji

Uwaga. – Informacje bezpieczeństwa pochodzące z dobrowolnych systemów zgłaszania zdarzeń dotyczących bezpieczeństwa są chronione, chyba że zastosowanie ma zasada stosowania wyjątków ochrony. Można to rozszerzyć na informacje bezpieczeństwa pochodzące z obowiązkowego systemu zgłaszania. Więcej informacji na temat ochrony danych dotyczących bezpieczeństwa, informacji dotyczących bezpieczeństwa i powiązanych źródeł znajduje się w Rozdziale 7.

8.6.8.1 Działania i publikacje związane z promocją bezpieczeństwa mogą również poprawić koordynację i współpracę pomiędzy różnymi organizacjami zaangażowanymi w nadzór nad bezpieczeństwem w danym Państwie. Dokument SSP i związane z nim polityki bezpieczeństwa i egzekwowania prawa mają zasadnicze znaczenie dla osiągnięcia integracji w zakresie szkoleń, komunikacji i rozpowszechniania powiązanych informacji. Organy regulacyjne Państwa odpowiedzialne za różne sektory lotnictwa, jak również inne niezależne podmioty, takie jak komisja badania wypadków, powinny mieć zintegrowane podejście do swoich odpowiednich ról w zakresie promowania bezpieczeństwa przez Państwo. Państwa powinny ustanowić formalne kanały komunikacji pomiędzy członkami Grupy koordynacyjnej SSP (podmioty państwowe zaangażowane we wdrażanie i utrzymanie SSP).

8.6.8.2 Z perspektywy operacyjnej, ważne jest, aby strategie operacyjne SSP, w tym informacje na temat zharmonizowanych wymagań w zakresie SMS i monitorowania odpowiednich podmiotów lotniczych, były udostępniane, komunikowane i koordynowane przez władze lotnicze Państw. Otwarty kanał komunikacyjny pozwoli uniknąć tworzenia sprzecznych wymagań w zakresie SMS lub kryteriów akceptacji dla różnych sektorów lotnictwa.

8.6.8.3 Przykłady informacji, które Państwa powinny uwzględnić w swojej wewnętrznej komunikacji i rozpowszechnianiu, obejmują:

- a) dokumentację, zasady i procedury SSP;
- b) wskaźniki SPI;
- c) informacje bezpieczeństwa w sektorze;
- d) profile ryzyka bezpieczeństwa organizacyjnego w sektorze;
- e) informacje w zakresie odpowiedzialności za bezpieczeństwo systemu;
- f) doświadczenia zdobyte w oparciu o wypadki i incydenty; oraz
- g) koncepcje i najlepsze praktyki zarządzania bezpieczeństwem.

8.6.8.4 Istnieje szczególna potrzeba skutecznej komunikacji w zakresie bezpieczeństwa, jeżeli podmioty lotnicze są zatwierdzone przez więcej niż jedno Państwo.

8.6.8.5 Istnieje wiele środków, które organizacje Państwa mogą przyjąć, aby ustanowić wewnętrzną komunikację w zakresie bezpieczeństwa, np. gazetki, biuletyny, ulotki, publikacje, seminaria, spotkania, szkolenia, strony internetowe, listy mailingowe, publikacje w mediach społecznościowych, dyskusje w grupach współpracy, itp.

8.6.8.6 Przy ocenie, jaki rodzaj mediów powinien być wykorzystany do przekazania konkretnego komunikatu, organizacja powinna ocenić, który z nich jest bardziej odpowiedni dla danego komunikatu i grupy docelowej. Dokumenty SSP mogą być publikowane na stronie internetowej, która jest łatwo dostępna dla personelu w sytuacji gdy dokumenty te są potrzebne. Inne informacje, takie jak zdobyte doświadczenia i najlepsze praktyki, mogą być bardziej odpowiednie dla okresowych wydań gazetki lub biuletynu.

8.6.8.7 Ustanowienie kampanii mających na celu zaradzenie szczególnym obawom lub zagrożeniom przy użyciu wielu mediów może być skuteczne w zwiększaniu świadomości problemu i zmianie nastawienia personelu.

8.6.9 Komunikacja zewnętrzna i rozpowszechnianie informacji bezpieczeństwa

8.6.9.1 Państwo powinno ustanowić odpowiednie platformy komunikacyjne lub media w celu ułatwienia wdrożenia SMS i poprawy kultury bezpieczeństwa całego systemu.

8.6.9.2 Podczas komunikowania się i rozpowszechniania informacji bezpieczeństwa na zewnątrz w obrębie branży lotniczej, oprócz pozycji przedstawionych w poprzedniej części, Państwa powinny również uwzględnić:

- a) materiały zawierające wytyczne w zakresie wdrożenia SMS;
- b) znaczenie zgłaszania;
- c) określenie dostępnych szkoleń z zakresu bezpieczeństwa dla społeczności lotniczej;
- d) promowanie wymiany informacji bezpieczeństwa:
 - 1) z podmiotami lotniczymi i pomiędzy nimi; oraz
 - 2) pomiędzy Państwami.

8.6.9.3 Dokumentacja SSP Państwa i powiązane polityki w zakresie bezpieczeństwa i egzekwowania przepisów powinny być również udostępniane podmiotom lotniczym.

8.6.9.4 Zasadniczo, te same media używane do komunikacji wewnętrznej mogą być używane zewnętrznie, o ile treść jest przydatna dla obu rodzajów odbiorców. Jednak w przypadku komunikacji zewnętrznej szczególną uwagę należy zwrócić na rozwiązania, które docierają do większej liczby odbiorców, w ramach, na przykład, mediów społecznościowych, biuletynów, list mailingowych, seminariów, tworząc społeczności branżowe do wymiany informacji bezpieczeństwa, a tym samym mnożąc zasięg wiadomości.

8.6.9.5 Państwa powinny promować tworzenie sieci udostępniania lub wymiany informacji bezpieczeństwa wśród społeczności lotniczej, chyba że prawo krajowe stanowi inaczej.

8.7. WDRÓŻENIE KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA

Podobnie jak w przypadku każdego wdrożenia większego projektu, wdrożenie SSP obejmuje wiele zadań i podzadań, które należy wykonać w określonym czasie. Liczba zadań, jak również zakres każdego zadania, zależy od dojrzałości krajowego systemu nadzoru nad bezpieczeństwem. W większości Państw, w opracowanie i wdrożenie SSP zaangażowanych jest kilka organizacji i podmiotów. Opracowanie planu wdrożenia może pomóc w złagodzeniu tego procesu. W niniejszym rozdziale przedstawiono poszczególne kroki poczynając od opracowania szczegółowego opisu systemu, uwarunkowań związanych ze skalowalnością, przeprowadzenia analizy luk do opracowania planu wdrożenia zawierającego zapewnienie ustanowienia solidnej podstawy SSP. Niniejsza część dotyczy również bieżącej oceny dojrzałości SSP.

8.7.1 Opis systemu lotnictwa cywilnego Państwa i kwestie dotyczące skalowalności

8.7.1.1 Zrozumienie wielkości i złożoności systemu lotniczego Państwa oraz interakcji pomiędzy poszczególnymi elementami ma zasadnicze znaczenie dla planowania SSP. Państwo musi wdrożyć SSP, ale sposób spełnienia wymagań będzie zależał od wielkości i złożoności systemu lotniczego. Więcej informacji na temat skalowalności znajduje się w Rozdziale 1.

8.7.1.2 SSP będzie również uwzględniał liczbę podmiotów lotniczych, ich wielkość i złożoność oraz środowisko regionalne. Państwa z niewielką liczbą podmiotów lotniczych powinny rozważyć ustanowienie partnerstw regionalnych. Partnerstwa regionalne z innymi Państwami lub za pośrednictwem regionalnych organizacji nadzoru nad bezpieczeństwem, dzielenie się zdobytymi doświadczeniami oraz informacjami o ryzyku bezpieczeństwa ograniczą do minimum wpływ przy jednoczesnym zwiększeniu korzyści wynikających z wdrożenia SSP.

8.7.1.3 Państwo powinno opisać system lotniczy oraz właściwe organy ds. lotnictwa w opisie systemu lotnictwa cywilnego. Powinien on obejmować przegląd struktur organizacyjnych i interfejsów. Jest to część procesu planowania wdrożenia SSP. Przegląd taki powinien zawierać opis następujących elementów:

- a) struktura istniejących ram prawnych w zakresie lotnictwa, w tym różne organy ds. lotnictwa funkcjonujące w Państwie;
- b) zakres obowiązków i odpowiedzialności związanych z zarządzaniem bezpieczeństwem różnych organów regulacyjnych;
- c) platforma lub mechanizm koordynacji SSP pomiędzy organizacjami; oraz
- d) wewnętrzny mechanizm przeglądu na poziomie Państwa i każdej organizacji.

8.7.2 Analiza luk i plan wdrożenia SSP

Analiza luk SSP

8.7.2.1 Analiza luk powinna być przeprowadzona przed opracowaniem planu wdrożenia SSP. Analiza luk ma na celu uzyskanie szczegółowych informacji na temat luk pomiędzy istniejącymi strukturami i procesami realizowanymi przez Państwo, a tymi wymaganymi do skutecznego wdrożenia SSP. W przypadku wielu Państw analiza luk pokazuje, że istnieje już znaczna zdolność zarządzania bezpieczeństwem. Wyzwaniem zazwyczaj jest udoskonalenie, wyrównanie i wzmocnienie tych istniejących możliwości. Elementy lub procesy określone jako wymagające działania stanowią bazę dla planu wdrożenia SSP.

Podstawa do wdrożenia SSP

8.7.2.2 Istotne jest, aby Państwa ustanowiły podstawę mającą stanowić wsparcie w skutecznym wdrożeniu SSP. Cele GASP wymagają od Państw stopniowego wdrażania skutecznych systemów nadzoru nad bezpieczeństwem, programu SSP oraz zaawansowanych możliwości zarządzania bezpieczeństwem niezbędnych do wsparcia przyszłych systemów lotniczych. Podstawa ta obejmuje aspekty dotyczące systemu nadzoru nad bezpieczeństwem, które są potrzebne do wsparcia podejścia opartego na większej wydajności.

8.7.2.3 Dane zebrane w ramach programu USOAP ICAO można wykorzystać do identyfikacji braków w tej podstawie. Odniesienie się do wszelkich niezadowolających pytań z list kontrolnych USOAP dotyczących kwestii związanych ze skutecznym wdrożeniem SSP (np. obowiązkowe systemy zgłaszania) powinno stanowić pierwszy krok we wdrażaniu SSP.

Plan wdrożenia SSP

8.7.2.4 Wdrożenie SSP ma na celu stopniowe ulepszanie istniejących procesów związanych z krajowym nadzorem nad bezpieczeństwem i zarządzaniem bezpieczeństwem. Odpowiednie zadania/podzadania są określane zgodnie z priorytetem i dokumentowane w planie działania. Plan wdrożenia SSP, wraz z dokumentem najwyższego szczebla w zakresie SSP, zapewniają „mapę drogową”, która wytycza działania Państwa w kierunku efektywnego SSP i ciągłej poprawy poziomu bezpieczeństwa. Te dwa kluczowe dokumenty powinny być łatwo dostępne dla wszystkich pracowników w celu zapewnienia, że wszystkie zaangażowane strony posiadają wiedzę na temat SSP i planów jego wdrożenia.

8.7.3 Ocena dojrzałości SSP

Wprowadzenie i cel

8.7.3.1 Ocena dojrzałości SSP powinna być przeprowadzona przy użyciu narzędzia stanowiącego odzwierciedlenie norm i zalecanych metod postępowania i materiałów zawierających wytyczne ICAO, opracowanego przez Państwo w celu spełnienia wymagań. Narzędzie powinno być wykorzystywane przez Państwa do przeprowadzania audytów wewnętrznych w celu ciągłego doskonalenia SSP. W stosownych przypadkach ICAO i inne podmioty zewnętrzne powinny również się do niego odwoływać. Narzędzie powinno opierać się na szeregu pytań (lub oczekiwań), z których Państwo może skorzystać aby ocenić skuteczność swojego SSP. Na ocenę dojrzałości SSP korzystnie wpłyną interakcje, takie jak bezpośrednie rozmowy i wywiady z udziałem wszystkich zainteresowanych stron. Narzędzie powinno być elastyczne i uwzględniać wielkość oraz złożoność krajowego systemu lotniczego.

Ocena

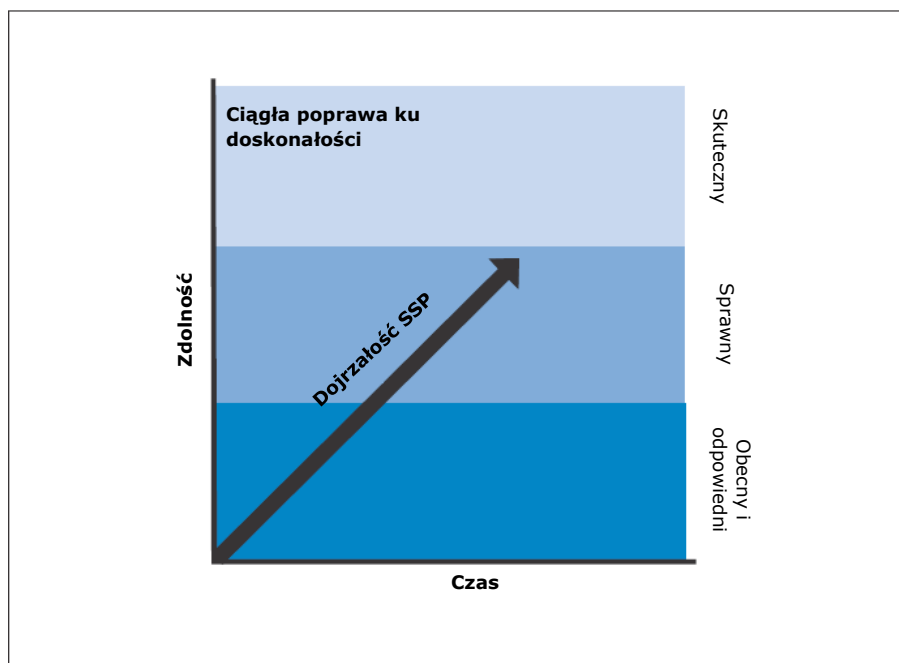
8.7.3.2 Po wdrożeniu podstawowych elementów SSP, można przeprowadzić ocenę dokumentacji. Ocena ma na celu ustalenie, czy przewidywania dotyczące zgodności i działania SSP są obecne i odpowiednie. Należy zebrać dowody na poparcie oceny. Na późniejszym etapie, można przeprowadzić ocenę SSP w celu zrozumienia do jakiego stopnia program działa i jest skuteczny w osiągnięciu celów. Skuteczność jest osiągnięta, kiedy wynik daje

za każdym razem pożądany rezultat. Zespół posiadający odpowiednie kompetencje w zakresie SSP i wiedzę techniczną zazwyczaj przeprowadza ocenę i zbiera dowody. Ważne jest, aby prowadzić ocenę w sposób umożliwiający interakcję z wieloma osobami na różnych poziomach organizacji w celu określenia skuteczności w całej organizacji. Na przykład określenie zakresu, w jakim polityka bezpieczeństwa została ogłoszona i zrozumiana przez personel, będzie wymagać interakcji z całym przekrojem personelu.

Bieżące monitorowanie i ciągłe doskonalenie

8.7.3.3 Państwo może wykorzystać to samo narzędzie do oceny skuteczności SSP podczas bieżącego monitorowania i ciągłego doskonalenia. Ocena prawdopodobnie zidentyfikuje zmiany w systemie lotniczym. W większości Państw wdrożenie SSP zajmie trochę czasu, a dojście do poziomu, na którym wszystkie elementy będą działać skutecznie, zajmie kilka lat. Rysunek 8-5 przedstawia różne poziomy dojrzałości SSP w miarę jak Państwo wdraża i rozwija program.

8.7.3.4 Ocena SSP może być przeprowadzona na różnych etapach, początkowo pod kątem obecności i przydatności kluczowych elementów. Na późniejszym etapie, SSP można poddać ocenie w celu zrozumienia, do jakiego stopnia działa i jest skuteczny w osiągnięciu celów. Państwa mogą okresowo przeprowadzać oceny w celu wsparcia ciągłego doskonalenia.



Rysunek 8-5. Schemat uzyskiwania dojrzałości SSP

ROZDZIAŁ 9

SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM (SMS)

9.1. WSTĘP

9.1.1 Niniejszy rozdział zawiera wytyczne dla podmiotów lotniczych w zakresie wdrożenia struktury systemu zarządzania bezpieczeństwem zgodnie z Załącznikiem 19 oraz wytyczne dla Państw w zakresie nadzoru nad systemem zarządzania bezpieczeństwem.

9.1.2 SMS ma na celu zapewnienie podmiotom lotniczym systematycznego podejścia do zarządzania bezpieczeństwem. Został on zaprojektowany w taki sposób, aby zapewnić ciągłą poprawę poziomu bezpieczeństwa poprzez identyfikację zagrożeń, zbieranie i analizę danych bezpieczeństwa i informacji bezpieczeństwa oraz ciągłą ocenę ryzyk bezpieczeństwa. SMS ma na celu proaktywne łagodzenie ryzyk bezpieczeństwa, zanim spowodują one wypadki i incydenty lotnicze. Pozwala on podmiotom lotniczym skutecznie zarządzać swoimi działaniami, poziomem bezpieczeństwa i zasobami, a jednocześnie lepiej rozumieć ich wkład w bezpieczeństwo lotnicze. Skuteczny SMS pokazuje Państwom zdolność podmiotu do zarządzania ryzykami bezpieczeństwa i umożliwia skuteczne zarządzanie bezpieczeństwem na poziomie Państwa.

9.1.3 Międzynarodowi operatorzy lotnictwa ogólnego powinni określić kryteria SMS, ustanowione przez Państwo rejestracji, w odniesieniu do statków powietrznych, które eksploatują oraz zapewnić, że ich SMS jest akceptowalny przez Państwo rejestracji. W celu ułatwienia akceptacji SMS, międzynarodowi operatorzy lotnictwa ogólnego powinni zwrócić się z zapytaniem do Państwa rejestracji, czy dozwolone jest stosowanie branżowego kodeksu praktyk.

9.1.4 Operatorzy dużych lub turboodrzutowych statków powietrznych w wielu Państwach rejestracji z AOC wydanym w zgodzie z Załącznikiem 6, Część I, są uznawani za podmioty lotnicze, dlatego SMS musi być akceptowany przez Państwo operatora.

9.2. STRUKTURA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM

9.2.1 Załącznik 19 określa strukturę wdrożenia i utrzymania SMS. Niezależnie od wielkości i złożoności podmiotu lotniczego, zastosowanie mają wszystkie elementy struktury SMS. Wdrożenie powinno być dostosowane do organizacji i zakresu jej działań.

9.2.2 Struktura SMS ICAO składa się z następujących czterech komponentów i dwunastu elementów:

Tabela 10. Komponenty i elementy struktury SMS ICAO

<i>KOMPONENT</i>		<i>ELEMENT</i>	
1.	Polityka bezpieczeństwa i jej cele	1.1	Zaangażowanie kierownictwa
		1.2	Odpowiedzialność i obowiązki w zakresie bezpieczeństwa
		1.3	Wyznaczenie personelu kluczowego dla bezpieczeństwa
		1.4	Koordinacja planowania reagowania awaryjnego
		1.5	Dokumentacja SMS
2.	Zarządzanie ryzykiem bezpieczeństwa	2.1	Identyfikacja zagrożeń
		2.2	Ocena ryzyka bezpieczeństwa i jego ograniczanie
3.	Zapewnianie bezpieczeństwa	3.1	Monitorowanie i pomiar poziomu bezpieczeństwa
		3.2	Zarządzanie zmianą
		3.3	Ciągłe doskonalenie systemu zarządzania bezpieczeństwem
4.	Promowanie bezpieczeństwa	4.1	Szkolenie i kształcenie
		4.2	Komunikacja w zakresie bezpieczeństwa

9.3. KOMPONENT NR 1: POLITYKA BEZPIECZEŃSTWA I JEJ CELE

9.3.1 Pierwszy komponent struktury SMS skupia się na tworzeniu środowiska, w którym zarządzanie bezpieczeństwem może być skuteczne. Opiera się na polityce i celach bezpieczeństwa, które określają zaangażowanie kierownictwa wyższego szczebla w bezpieczeństwo, jego cele i wspierającą strukturę organizacyjną.

9.3.2 Zaangażowanie kierownictwa i przywództwo w zakresie bezpieczeństwa jest kluczowym elementem wdrożenia skutecznego systemu SMS oraz jest potwierdzane poprzez politykę bezpieczeństwa i ustanowienie celów bezpieczeństwa. Zaangażowanie kierownictwa w bezpieczeństwo jest demonstrowane poprzez podejmowanie decyzji i przydzielanie zasobów. Te decyzje i działania powinny być zawsze zgodne z polityką i celami bezpieczeństwa w celu kultywowania pozytywnej kultury bezpieczeństwa.

9.3.3 Polityka bezpieczeństwa powinna być opracowana i zatwierdzona przez kierownictwo wyższego szczebla i podpisana przez dyrektora odpowiedzialnego. Podczas opracowywania polityki bezpieczeństwa i celów bezpieczeństwa należy konsultować się z kluczowymi pracownikami ds. bezpieczeństwa oraz, w stosownych przypadkach, organami reprezentującymi pracowników (fora pracowników, związki zawodowe) w celu promowania poczucie wspólnej odpowiedzialności.

9.3.4 Zaangażowanie kierownictwa

Polityka bezpieczeństwa

9.3.4.1 Polityka bezpieczeństwa powinna być wyraźnie popierana przez kierownictwo wyższego szczebla i dyrektora odpowiedzialnego. „Wyraźne poparcie” odnosi się do aktywnego wsparcia polityki bezpieczeństwa przez kierownictwo w sposób widoczny dla reszty organizacji. Można to zrobić za pomocą wszelkich środków komunikacji oraz poprzez dostosowanie działań do polityki bezpieczeństwa.

9.3.4.2 Obowiązkiem kierownictwa jest rozpowszechnianie polityki bezpieczeństwa w całej organizacji w celu zapewnienia, że wszyscy pracownicy rozumieją politykę bezpieczeństwa i działają zgodnie z jej założeniami.

9.3.4.3 W celu odzwierciedlenia zaangażowania organizacji w bezpieczeństwo, polityka bezpieczeństwa powinna zawierać zobowiązanie do:

- a) ciągłej poprawy poziomu bezpieczeństwa;
- b) promowania i utrzymywania pozytywnej kultury bezpieczeństwa w organizacji;

- c) zachowania zgodności ze wszystkimi obowiązującymi wymaganiami prawnymi;
- d) zapewnienia zasobów niezbędnych do dostarczenia bezpiecznego produktu lub usługi;
- e) zapewnienia, że bezpieczeństwo jest głównym obowiązkiem wszystkich kierowników; oraz
- f) zapewnienia, że jest ona zrozumiała, wdrożona i utrzymywana na wszystkich szczeblach.

9.3.4.4 Polityka bezpieczeństwa powinna również odnosić się do systemu zgłaszania zdarzeń dotyczących bezpieczeństwa w celu zachęcenia do zgłaszania problemów związanych z bezpieczeństwem oraz informowania pracowników o polityce dyscyplinarnej stosowanej w przypadku wydarzeń lub problemów związanych z bezpieczeństwem, które są zgłaszane.

9.3.4.5 Polityka dyscyplinarna jest stosowana w celu ustalenia czy wystąpił błąd lub złamanie przepisów, aby organizacja mogła ustalić, czy należy podjąć jakiegokolwiek działania dyscyplinarne. Aby zapewnić sprawiedliwe traktowanie osób zaangażowanych, istotne jest, aby osoby odpowiedzialne za dokonanie takiego ustalenia posiadały niezbędną wiedzę techniczną, tak aby kontekst wydarzenia mógł być w pełni rozważony.

9.3.4.6 Polityka ochrony danych bezpieczeństwa i informacji bezpieczeństwa, a także osób składających zgłoszenia, mogą mieć pozytywny wpływ na kulturę zgłaszania. Podmiot lotniczy oraz Państwo powinni zapewnić pozbawienie cech umożliwiających identyfikację oraz agregację raportów, aby umożliwić przeprowadzenie analiz bezpieczeństwa bez konieczności angażowania personelu lub konkretnych podmiotów lotniczych. Ponieważ znaczące zdarzenia mogą wywoływać procesy i procedury poza zakresem systemu SMS podmiotu lotniczego, właściwy organ Państwa może nie wydać zgody na wczesne pozbawienie raportów elementów umożliwiających identyfikację we wszystkich okolicznościach. Niemniej jednak polityka pozwalająca na odpowiednie pozbawienie raportów elementów umożliwiających identyfikację może poprawić jakość zbieranych danych.

Cele bezpieczeństwa

9.3.4.7 Biorąc pod uwagę politykę bezpieczeństwa, podmiot lotniczy powinien również ustanowić cele bezpieczeństwa, aby określić, co zamierza osiągnąć w odniesieniu do wyników bezpieczeństwa. Cele bezpieczeństwa powinny być krótkimi, ogólnymi stwierdzeniami dotyczącymi priorytetów w zakresie bezpieczeństwa organizacji oraz powinny dotyczyć najbardziej istotnych ryzyk bezpieczeństwa. Cele bezpieczeństwa mogą być zawarte w polityce bezpieczeństwa (lub udokumentowane osobno) i powinny określać, co organizacja zamierza osiągnąć w zakresie bezpieczeństwa. Do monitorowania postępów w osiągnięciu tych celów potrzebne są wskaźniki poziomu bezpieczeństwa (SPI) i cele wskaźników poziomu bezpieczeństwa (SPT), które zostały omówione w dalszej części niniejszego Rozdziału w Komponentcie 3.

9.3.4.8 Polityka bezpieczeństwa i cele bezpieczeństwa powinny być poddawane okresowym przeglądom w celu zapewnienia ich aktualności (np. przegląd wymagany będzie w przypadku zmiany na stanowisku dyrektora odpowiedzialnego).

9.3.5 Odpowiedzialność i obowiązki w zakresie bezpieczeństwa

Dyrektor odpowiedzialny

9.3.5.1 Dyrektor odpowiedzialny, zazwyczaj dyrektor generalny, jest osobą, która ma najwyższe uprawnienia w zakresie bezpiecznego działania organizacji. Dyrektor odpowiedzialny ustanawia i promuje politykę bezpieczeństwa i cele bezpieczeństwa, które przedstawiają bezpieczeństwo jako podstawową wartość organizacji. Powinien on mieć uprawnienia do podejmowania decyzji w imieniu organizacji, kontrolowania zasobów, zarówno finansowych, jak i ludzkich, odpowiadać za zapewnienie, że podejmowane są działania mające na celu rozstrzygnięcie problemów związanych z bezpieczeństwem i ryzyk bezpieczeństwa oraz powinien mieć obowiązek reagowania na wypadki i incydenty.

9.3.5.2 Podmioty lotnicze mogą napotkać problemy z określeniem najwłaściwszej osoby do pełnienia funkcji dyrektora odpowiedzialnego, zwłaszcza w dużych złożonych organizacjach z wieloma podmiotami i wieloma certyfikatami, upoważnieniami lub zatwierdzeniami. Ważne jest, aby wybrana osoba była usytuowana na najwyższym szczeblu organizacji, zapewniając w ten sposób podejmowanie odpowiednich strategicznych decyzji dotyczących bezpieczeństwa.

9.3.5.3 Podmiot lotniczy musi wyznaczyć dyrektora odpowiedzialnego, nakładając obowiązki związane z ogólnym poziomem bezpieczeństwa na szczeblu organizacji, z uprawnieniami do podejmowania działań w celu zapewnienia skuteczności SMS. Należy określić odpowiedzialność wszystkich członków kierownictwa w zakresie bezpieczeństwa, a ich rola w odniesieniu do SMS powinna odzwierciedlać sposób, w jaki mogą przyczynić się do pozytywnej kultury bezpieczeństwa. Zakres obowiązków, odpowiedzialności i uprawnień związanych z bezpieczeństwem powinien być udokumentowany i rozpowszechniony w całej organizacji. Odpowiedzialność kierowników w zakresie bezpieczeństwa powinna obejmować alokację zasobów ludzkich, technicznych, finansowych lub innych niezbędnych do skutecznego i wydajnego działania SMS.

Uwaga. – Termin „odpowiedzialność” odnosi się do zobowiązań, których nie można delegować. Termin „obowiązki” odnosi się do funkcji i działań, które mogą być delegowane.

9.3.5.4 W przypadku, gdy SMS dotyczy kilku różnych certyfikatów, upoważnień lub zatwierdzeń będących częścią tego samego podmiotu prawnego, powinien funkcjonować jeden dyrektor odpowiedzialny. Tam, gdzie nie jest to możliwe, należy wyznaczyć poszczególnych dyrektorów odpowiedzialnych za każdy certyfikat, upoważnienie lub zatwierdzenie organizacji oraz określić jasne zakresy odpowiedzialności. Ważne jest również, aby określić, w jaki sposób ich zakresy odpowiedzialności za bezpieczeństwo będą koordynowane.

9.3.5.5 Jednym z najskuteczniejszych sposobów widocznego zaangażowania dyrektora odpowiedzialnego jest prowadzenie regularnych spotkań z zakresu bezpieczeństwa. Ponieważ dyrektor odpowiedzialny jest odpowiedzialny za bezpieczeństwo organizacji, aktywny udział w tych spotkaniach pozwala mu na:

- a) przegląd celów bezpieczeństwa;
- b) monitorowanie poziomu bezpieczeństwa i postępów w osiąganiu poziomów docelowych;
- c) podejmowanie na czas decyzji dotyczących bezpieczeństwa;
- d) alokację odpowiednich zasobów;
- e) rozliczać kierowników z ich obowiązków w zakresie bezpieczeństwa, terminów wykonania i wdrożenia; oraz
- f) bycie postrzeganym przez cały personel jako osoba, która jest zainteresowana i odpowiedzialna za bezpieczeństwo.

9.3.5.6 Dyrektor odpowiedzialny nie jest zazwyczaj zaangażowany w codzienne działania organizacji lub problemy w miejscu pracy, ale powinien zapewnić odpowiednią strukturę organizacyjną do zarządzania i obsługi SMS. Obowiązki związane z zarządzaniem bezpieczeństwem są często delegowane do kierownictwa wyższego szczebla i innych kluczowych pracowników ds. bezpieczeństwa. Chociaż obowiązki związane z codziennym działaniem systemu SMS można delegować, dyrektor odpowiedzialny nie może delegować odpowiedzialności za system, ani za podejmowanie decyzji dotyczących ryzyka bezpieczeństwa. Na przykład następujące kwestie związane z odpowiedzialnością w zakresie bezpieczeństwa nie mogą być delegowane

- a) zapewnienie, że polityka bezpieczeństwa jest odpowiednia i jest rozpowszechniona;
- b) zapewnienie niezbędnej alokacji zasobów (finansowanie, personel, szkolenie, zakupy); oraz

- c) ustalenie akceptowalnych limitów ryzyka bezpieczeństwa i zapewnienie niezbędnych środków kontroli.

9.3.5.7 Właściwe jest, aby dyrektor odpowiedzialny posiadał odpowiedzialność w zakresie bezpieczeństwa w odniesieniu do następujących kwestii:

- a) zapewnienie wystarczających zasobów finansowych i ludzkich do wdrożenia skutecznego systemu SMS;
- b) promowanie pozytywnej kultury bezpieczeństwa;
- c) ustanowienie i promowanie polityki bezpieczeństwa;
- d) ustanowienie celów bezpieczeństwa organizacji;
- e) zapewnienie, że SMS jest prawidłowo wdrożony i spełnia wymagania; oraz
- f) ciągłe doskonalenie systemu SMS.

9.3.5.8 Uprawnienia dyrektora odpowiedzialnego obejmują, między innymi, posiadanie ostatecznego uprawnienia:

- a) do rozwiązywania wszystkich problemów związanych z bezpieczeństwem; oraz
- b) nad operacjami realizowanymi na podstawie certyfikatu, upoważnienia lub zatwierdzenia organizacji, w tym uprawnienie do wstrzymania operacji lub działania.

9.3.5.9 Należy określić uprawnienia do podejmowania decyzji dotyczących tolerancji ryzyka bezpieczeństwa. Dotyczy to osób, które mogą podejmować decyzje dotyczące akceptowalności ryzyka, a także uprawnienia do wyrażenia zgody na wprowadzenie zmiany. Uprawnienia mogą być przypisane osobie, stanowisku kierowniczemu lub komitetowi.

9.3.5.10 Uprawnienia do podejmowania decyzji dotyczących tolerancji ryzyka bezpieczeństwa powinny być współmierne do uprawnienia do podejmowania decyzji i przydzielania zasobów przez kierownika. Kierownik niższego szczebla (lub grupa zarządzająca) może być upoważniony do podejmowania decyzji dotyczących tolerancji do pewnego poziomu. Poziomy ryzyka przekraczające uprawnienia kierownika muszą być przekazane do rozpatrzenia przez wyższy szczebel kierownictwa z większymi uprawnieniami.

Odpowiedzialność i obowiązki

9.3.5.11 Odpowiedzialność i obowiązki wszystkich pracowników, kierownictwa i personelu zaangażowanych w obowiązki związane z bezpieczeństwem wspierające zapewnianie bezpiecznych produktów i operacji powinny być jasno określone. Obowiązki w zakresie bezpieczeństwa powinny koncentrować się na wkładzie pracownika w bezpieczeństwo organizacji (wyniki bezpieczeństwa organizacji). Zarządzanie bezpieczeństwem jest podstawową funkcją; jako taki każdy kierownik wyższego szczebla ma pewien stopień zaangażowania w działanie SMS.

9.3.5.12 Wszystkie zdefiniowane odpowiedzialności, obowiązki i uprawnienia powinny być określone w dokumentacji SMS podmiotu lotniczego i powinny być rozpowszechnione w całej organizacji. Odpowiedzialność i obowiązki w zakresie bezpieczeństwa każdego kierownika wyższego szczebla stanowią integralny element jego opisu stanowiska. Opis powinien również zawierać różne funkcje zarządzania bezpieczeństwem pomiędzy kierownikami liniowymi a kierownikiem ds. bezpieczeństwa (w celu uzyskania dodatkowych informacji, patrz pkt 9.3.6).

9.3.5.13 Odpowiedzialność w zakresie bezpieczeństwa w całej organizacji i sposób jej definiowania będą zależały od rodzaju i złożoności organizacji oraz preferowanych metod komunikacji. Zwykle odpowiedzialność i

obowiązki w zakresie bezpieczeństwa będą odzwierciedlone na schematach organizacyjnych, dokumentach określających obowiązki poszczególnych departamentów oraz w opisach stanowisk pracowników.

9.3.5.14 Podmiot lotniczy powinien dążyć do unikania konfliktów interesów pomiędzy obowiązkami pracowników w zakresie bezpieczeństwa a innymi obowiązkami organizacyjnymi. Przydzielenie odpowiedzialności i obowiązków związanych z systemem SMS powinno być zorganizowane w taki sposób, aby ograniczyć do minimum przypadki ich nakładania się i/lub występowania luk.

Odpowiedzialność i obowiązki w odniesieniu do organizacji zewnętrznych

9.3.5.15 Podmiot lotniczy jest odpowiedzialny za poziom bezpieczeństwa organizacji zewnętrznych, w których istnieje interfejs SMS. Podmiot może zostać pociągnięty do odpowiedzialności za poziom bezpieczeństwa produktów lub usług świadczonych przez organizacje zewnętrzne wspierające jego działalność, nawet jeżeli od organizacji zewnętrznych nie wymaga się posiadania systemu SMS. Istotne jest, aby system SMS podmiotu lotniczego współdziałał z systemami bezpieczeństwa wszystkich organizacji zewnętrznych, które przyczyniają się do bezpiecznego zapewniania produktów lub usług.

9.3.6 Wyznaczenie personelu kluczowego dla bezpieczeństwa

9.3.6.1 Wyznaczenie kompetentnej osoby lub osób do pełnienia roli kierownika ds. bezpieczeństwa jest niezbędne do skutecznego wdrożenia i funkcjonowania systemu SMS. Kierownik ds. bezpieczeństwa może być określany różnymi tytułami. Dla celów niniejszego podręcznika stosowany jest ogólny termin „kierownik ds. bezpieczeństwa”, który odnosi się do funkcji, niekoniecznie do jednostki. Osoba pełniąca funkcję kierownika ds. bezpieczeństwa odpowiada przed dyrektorem odpowiedzialnym za działanie systemu SMS oraz za świadczenie usług w zakresie bezpieczeństwa innym komórkom organizacji.

9.3.6.2 Kierownik ds. bezpieczeństwa doradza dyrektorowi odpowiedzialnemu i kierownikom liniowym w sprawach związanych z zarządzaniem bezpieczeństwem oraz odpowiada za koordynowanie i rozpowszechnianie problemów związanych z bezpieczeństwem w obrębie organizacji, jak również wśród zewnętrznych członków społeczności lotniczej. Funkcje kierownika ds. bezpieczeństwa obejmują między innymi:

- a) zarządzanie planem wdrożenia systemu SMS w imieniu dyrektora odpowiedzialnego (po wstępnym wdrożeniu);
- b) prowadzenie/ułatwianie identyfikacji zagrożeń i analizy ryzyka bezpieczeństwa;
- c) monitorowanie działań naprawczych i ocenę ich wyników;
- d) dostarczanie okresowych raportów na temat poziomu bezpieczeństwa organizacji;
- e) prowadzenie dokumentacji i rejestrów związanych z SMS;
- f) planowanie i ułatwianie szkoleń pracowników w zakresie bezpieczeństwa;
- g) zapewnianie niezależnego doradztwa w sprawach związanych z bezpieczeństwem;
- h) monitorowanie obaw dotyczących bezpieczeństwa w branży lotniczej i ich postrzeganego wpływu na operacje organizacji mające na celu zapewnianie produktów i usług; oraz
- i) koordynacja i komunikacja (w imieniu dyrektora odpowiedzialnego) z władzami lotnictwa cywilnego i innymi organami Państwa, w razie potrzeby, w kwestiach związanych z bezpieczeństwem.

9.3.6.3 W większości organizacji na kierownika ds. bezpieczeństwa wyznaczana jest konkretna osoba. W zależności od wielkości, charakteru i złożoności organizacji rola kierownika ds. bezpieczeństwa może być jedyną sprawowaną funkcją lub może być łączona z innymi zadaniami. Ponadto, niektóre organizacje mogą potrzebować

przypisać tą funkcję grupie osób. Organizacja musi zapewnić, że wybrana opcja nie spowoduje żadnych konfliktów interesów. Tam, gdzie jest to możliwe, kierownik ds. bezpieczeństwa nie powinien być bezpośrednio zaangażowany w zapewnianie produktu lub usługi, ale powinien posiadać praktyczną wiedzę na ich temat. Nominacja powinna również uwzględniać potencjalne konflikty interesów z innymi zadaniami i funkcjami. Takie konflikty interesów mogą obejmować:

- a) konkurowanie o finansowanie (np. kierownik finansowy będący kierownikiem ds. bezpieczeństwa);
- b) sprzeczne priorytety dotyczące zasobów; oraz
- c) pełnienie przez kierownika ds. bezpieczeństwa roli operacyjnej oraz prowadzenie oceny skuteczności systemu SMS w działaniach operacyjnych, w które zaangażowany jest kierownik ds. bezpieczeństwa.

9.3.6.4 W przypadku, gdy funkcja ta jest przydzielona grupie osób (np. gdy podmioty lotnicze rozszerzają system SMS na wiele rodzajów działalności), jedna z osób powinna zostać wyznaczona jako kierownik „wiodący” ds. bezpieczeństwa w celu utrzymania bezpośredniego i jasnego kanału raportowania do dyrektora odpowiedzialnego.

9.3.6.5 Kompetencje kierownika ds. bezpieczeństwa powinny obejmować, między innymi:

- a) doświadczenie w zarządzaniu bezpieczeństwem/jakością;
- b) doświadczenie operacyjne związane z produktem lub usługą zapewnianą przez organizację;
- c) doświadczenie techniczne pozwalające zrozumieć systemy, które wspierają operacje lub zapewniany produkt/usługę;
- d) umiejętności interpersonalne;
- e) umiejętności analityczne i rozwiązywania problemów;
- f) umiejętności zarządzania projektami;
- g) umiejętności komunikacji ustnej i pisemnej; oraz
- h) zrozumienie czynników ludzkich.

9.3.6.6 W zależności od wielkości, charakteru i złożoności organizacji, kierownik ds. bezpieczeństwa może być wspierany przez dodatkowy personel. Kierownik ds. bezpieczeństwa i personel pomocniczy odpowiadają za zapewnienie sprawnego gromadzenia i analizowania danych dotyczących bezpieczeństwa oraz odpowiedniego rozpowszechniania w ramach organizacji powiązanych informacji dotyczących bezpieczeństwa, tak aby można było podejmować decyzje i stosować środki kontroli ryzyka bezpieczeństwa.

9.3.6.7 Podmioty lotnicze powinny ustanowić odpowiednie komitety ds. bezpieczeństwa, które wspierają funkcje SMS w całej organizacji. Powinny one określić skład komitetu ds. bezpieczeństwa i częstotliwość spotkań.

9.3.6.8 Komitet ds. bezpieczeństwa najwyższego szczebla, czasami określany jako Komisja ds. przeglądu bezpieczeństwa (SRB), posiada w swoim składzie dyrektora odpowiedzialnego i kierowników wyższego szczebla z kierownikiem ds. bezpieczeństwa uczestniczącym w charakterze doradczym. SRB ma charakter strategiczny i zajmuje się kwestiami związanymi z polityką bezpieczeństwa, alokacją zasobów i działaniem organizacji. SRB monitoruje:

- a) skuteczność systemu SMS;
- b) terminową reakcję we wdrażaniu niezbędnych działań w zakresie środków kontroli ryzyka bezpieczeństwa;

- c) poziom bezpieczeństwa w stosunku do polityki i celów bezpieczeństwa organizacji;
- d) ogólną skuteczność strategii łagodzenia ryzyka bezpieczeństwa;
- e) skuteczność procesów zarządzania bezpieczeństwem organizacji, które wspierają:
 - 1) deklarowany priorytet organizacji w zakresie zarządzania bezpieczeństwem; oraz
 - 2) promowanie bezpieczeństwa w całej organizacji.

9.3.6.9 Po określeniu kierunku strategicznego przez komitet ds. bezpieczeństwa najwyższego szczebla, należy wdrożyć strategię bezpieczeństwa w całej organizacji. Można to osiągnąć poprzez tworzenie grup ds. działań związanych z bezpieczeństwem (SAG), które skupiają się głównie na kwestiach operacyjnych. W skład SAG wchodzi zazwyczaj kierownicy oraz personel z pierwszej linii, a przewodniczy jej wyznaczony kierownik. SAG to jednostki taktyczne, które zajmują się konkretnymi problemami związanymi z wdrożeniem działań zgodnie ze strategiami opracowanymi przez Komisję ds. przeglądu bezpieczeństwa (SRB). Grupy ds. działań związanych z bezpieczeństwem:

- a) monitorują poziom bezpieczeństwa operacyjnego w obszarach funkcjonalnych organizacji i zapewniają, że prowadzone są odpowiednie działania związane z zarządzaniem ryzykiem bezpieczeństwa;
- b) dokonują przeglądu dostępnych danych dotyczących bezpieczeństwa i decydują o wdrożeniu odpowiednich strategii w zakresie środków kontroli ryzyka bezpieczeństwa oraz zapewniają informacje zwrotne dla pracowników;
- c) oceniają wpływ na bezpieczeństwo związany z wprowadzeniem zmian operacyjnych lub nowych technologii;
- d) koordynują wdrażanie wszelkich działań związanych ze środkami kontroli ryzyka bezpieczeństwa i zapewniają szybkie podejmowanie działań; oraz
- e) dokonują przeglądu skuteczności konkretnych środków kontroli ryzyka bezpieczeństwa.

9.3.7 Koordynacja planowania reagowania awaryjnego

9.3.7.1 Z definicji, sytuacja awaryjna to nagła, nieplanowana sytuacja lub zdarzenie wymagające natychmiastowego działania. Koordynacja planowania reagowania awaryjnego odnosi się do planowania działań, które mają miejsce w ograniczonym czasie podczas nieplanowanej sytuacji awaryjnej w lotnictwie. Plan reagowania awaryjnego (ERP) stanowi integralny element procesu SRM podmiotu lotniczego mający na celu reagowanie na sytuacje awaryjne, kryzysy lub zdarzenia związane z lotnictwem. W przypadku wystąpienia sytuacji, w której operacje lub działania lotnicze podmiotu lotniczego są zagrożone przez sytuacje awaryjne, takie jak sytuacja zagrożenia zdrowia publicznego/pandemia, scenariusze te powinny również zostać uwzględnione w ERP, stosownie do przypadku. ERP powinien uwzględniać przewidywalne sytuacje awaryjne określone w SMS i obejmować działania łagodzące, procesy i środki kontroli w celu skutecznego zarządzania sytuacjami awaryjnymi związanymi z lotnictwem.

9.3.7.2 Ogólnym celem ERP jest bezpieczna kontynuacja operacji i jak najszybszy powrót do normalnych działań. Powinien on zapewniać uporządkowane i skuteczne przejście z operacji normalnych do działań awaryjnych, w tym przydzielenie obowiązków w sytuacji awaryjnej i delegowanie uprawnień. Obejmuje okres czasu wymagany do przywrócenia „normalnych” operacji po wystąpieniu sytuacji awaryjnej. ERP określa działania, które powinien podjąć odpowiedzialny personel w sytuacji awaryjnej. Większość sytuacji awaryjnych będzie wymagała skoordynowanych działań różnych organizacji, być może z innymi podmiotami lotniczymi oraz innymi organizacjami

zewnętrznymi, takimi jak służby ratownicze niezwiązane z lotnictwem. ERP powinien być łatwo dostępny dla odpowiedniego kluczowego personelu, jak również dla zewnętrznych organizacji koordynujących.

9.3.7.3 Koordynacja planowania reagowania awaryjnego dotyczy tylko tych podmiotów lotniczych, które są zobowiązane do ustanowienia i utrzymania ERP. Załącznik 19 nie wymaga tworzenia lub opracowywania ERP, planowanie reagowania awaryjnego ma zastosowanie tylko do określonych podmiotów lotniczych wskazanych w odpowiednich Załącznikach ICAO (różne przepisy dotyczące postępowania w sytuacjach awaryjnych mogą być stosowane w innych Załącznikach). Koordynacja ta powinna być wykonywana w ramach okresowych testów planu reagowania awaryjnego.

9.3.8 Dokumentacja SMS

9.3.8.1 Dokumentacja SMS powinna obejmować „podręcznik SMS”, który opisuje polityki, procesy i procedury SMS podmiotu lotniczego w celu ułatwienia wewnętrznej administracji, komunikacji i utrzymania SMS w danej organizacji. Dokumentacja powinna pomagać personelowi w zrozumieniu sposobu działania systemu SMS organizacji i osiągnięcia założeń polityki i celów bezpieczeństwa. Dokumentacja powinna zawierać opis systemu, który określa zakres działania SMS. Powinna także pomagać w wyjaśnianiu związku pomiędzy różnymi politykami, procesami, procedurami i praktykami oraz określać sposób, w jaki łączą się one z polityką i celami bezpieczeństwa podmiotu lotniczego. Dokumentacja powinna być dostosowana i napisana w taki sposób, aby uwzględniać codzienne działania związane z zarządzaniem bezpieczeństwem, które mogą być łatwo zrozumiane przez personel w całej organizacji.

9.3.8.2 Podręcznik SMS służy również jako podstawowe narzędzie komunikacji w zakresie bezpieczeństwa pomiędzy podmiotem lotniczym a kluczowymi zainteresowanymi stronami (np. władze lotnictwa cywilnego w celu akceptacji przepisów, oceny i późniejszego monitorowania SMS). Podręcznik SMS może być samodzielnym dokumentem lub może być zintegrowany z innymi dokumentami organizacyjnymi (lub dokumentacją) prowadzonymi przez podmiot lotniczy. Jeżeli szczegółowe informacje dotyczące procesów SMS organizacji zostały już uwzględnione w istniejących dokumentach, wystarczy odpowiednie odniesienie do takich dokumentów. Podręcznik SMS musi być aktualizowany. Ponieważ jest to dokument podlegający kontroli, przed wprowadzeniem istotnych zmian w podręczniku SMS, może być wymagana zgoda władzy lotnictwa cywilnego.

9.3.8.3 Podręcznik SMS powinien zawierać szczegółowy opis polityk, procesów i procedur podmiotu lotniczego, w tym:

- a) politykę bezpieczeństwa i cele bezpieczeństwa;
- b) odniesienie do wszelkich obowiązujących wymogów prawnych w zakresie SMS;
- c) opis systemu;
- d) odpowiedzialność w zakresie bezpieczeństwa i kluczowy personel bezpieczeństwa;
- e) procesy i procedury dotyczące dobrowolnego i obowiązkowego systemu zgłaszania zdarzeń dotyczących bezpieczeństwa;
- f) procesy i procedury identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa;
- g) procedury badań bezpieczeństwa;
- h) procedury ustanawiania i monitorowania wskaźników poziomu bezpieczeństwa;
- i) procesy i procedury szkolenia w zakresie SMS oraz kwestie związane z komunikacją;
- j) procesy i procedury komunikacji w zakresie bezpieczeństwa;

- k) procedury audytu wewnętrznego;
- l) procedury zarządzania zmianą;
- m) procedury zarządzania dokumentacją SMS; oraz
- n) w stosownych przypadkach, koordynacja planowania reagowania awaryjnego.

9.3.8.4 Dokumentacja SMS obejmuje również kompilację i utrzymywanie rejestrów operacyjnych potwierdzających istnienie i bieżące działanie systemu SMS. Rejestry operacyjne to wyniki procesów i procedur SMS, takich jak zarządzanie ryzykiem bezpieczeństwa i zapewnianie bezpieczeństwa. Rejestry operacyjne SMS powinny być przechowywane zgodnie z obowiązującymi okresami przechowywania. Typowe rejestry operacyjne SMS powinny obejmować:

- a) rejestr zagrożeń i raporty o zagrożeniach/bezpieczeństwie;
- b) SPI i powiązane mapy;
- c) rejestr zakończonych ocen ryzyka bezpieczeństwa;
- d) rejestry z wewnętrznych przeglądów lub audytów;
- e) rejestry audytu wewnętrznego;
- f) rejestry SMS/rejestry szkoleń w zakresie bezpieczeństwa;
- g) protokoły posiedzeń komitetu ds. SMS/bezpieczeństwa;
- h) plan wdrożenia SMS (podczas wstępnego wdrożenia); oraz
- i) analiza luk mająca na celu wsparcie planu wdrożenia.

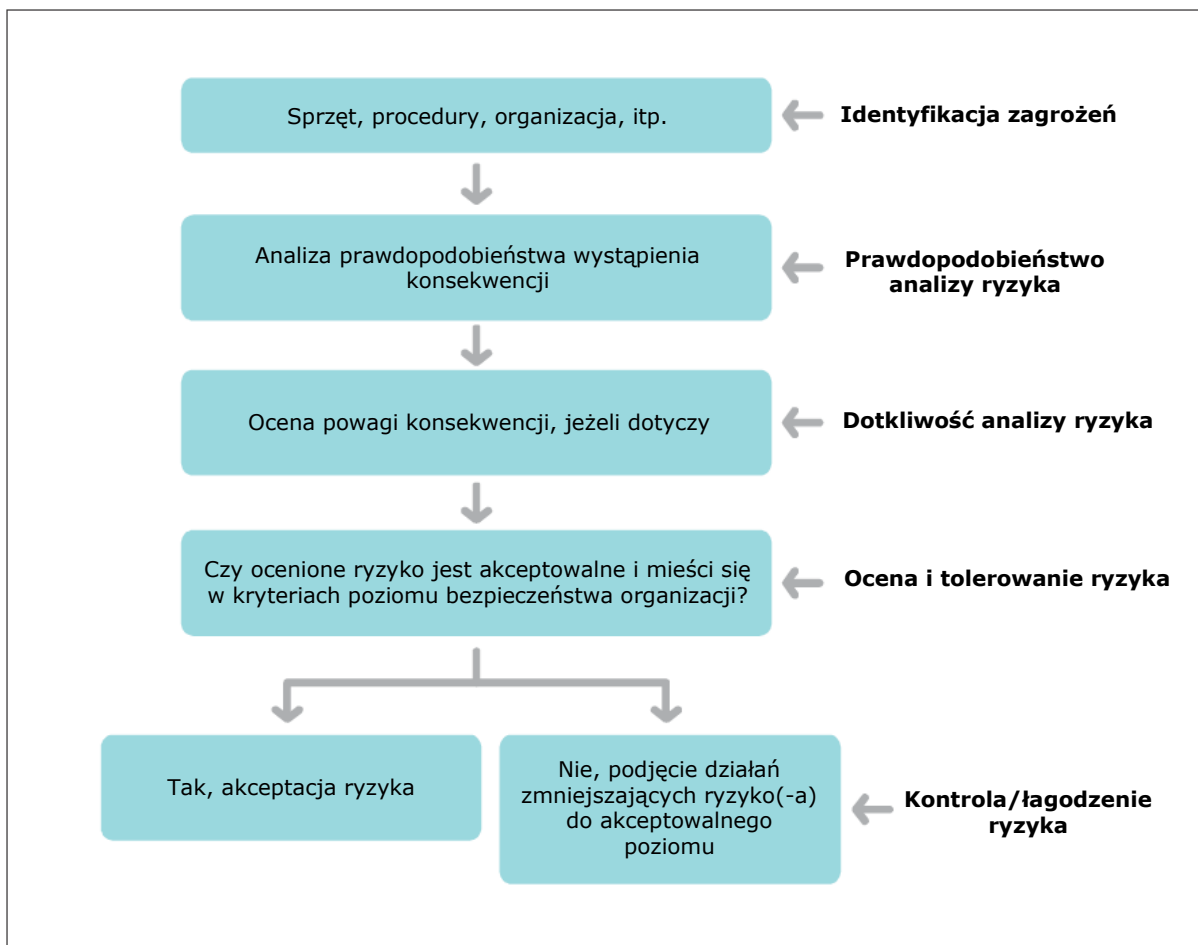
9.4. KOMPONENT NR 2: ZARZĄDZANIE RYZYKIEM BEZPIECZEŃSTWA

9.4.1 Podmioty lotnicze powinny zapewnić, że zarządzają swoimi ryzykami bezpieczeństwa. Proces ten jest znany jako zarządzanie ryzykiem bezpieczeństwa (SRM), i obejmuje identyfikację zagrożeń, ocenę ryzyka bezpieczeństwa oraz łagodzenie ryzyka bezpieczeństwa.

9.4.2 Proces SRM w sposób systematyczny identyfikuje zagrożenia występujące w kontekście zapewniania produktów lub usług. Zagrożenia mogą wynikać z niedoskonałości systemów w odniesieniu do projektu, funkcji technicznych, interfejsu ludzkiego lub interakcji z innymi procesami i systemami. Mogą również wynikać z niedostosowania istniejących procesów lub systemów do zmian w środowisku operacyjnym podmiotu lotniczego. Dokładna analiza tych czynników może często prowadzić do identyfikacji potencjalnych zagrożeń w dowolnym momencie cyklu eksploatacji lub działania.

9.4.3 Zrozumienie systemu i jego środowiska pracy jest niezbędne do osiągnięcia wysokiego poziomu bezpieczeństwa. Szczegółowy opis systemu, który definiuje system i jego interfejsy, będzie pomocny. Zagrożenia mogą być identyfikowane w ciągu całego cyklu eksploatacyjnego na podstawie źródeł wewnętrznych i zewnętrznych. Oceny ryzyka bezpieczeństwa i łagodzenie ryzyka bezpieczeństwa będą musiały być przedmiotem stałych przeglądów w celu zapewnienia skuteczności. Rysunek 9-1 przedstawia schemat procesu identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa podmiotu lotniczego.

Uwaga. – Szczegółowe wytyczne w zakresie procedur identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa zostały przedstawione w Rozdziale 2.



Rysunek 9-1. Proces identyfikacji zagrożeń i zarządzania ryzykiem

9.4.4 Identyfikacja zagrożeń

Identyfikacja zagrożeń stanowi pierwszy etap w procesie SRM. Podmiot lotniczy powinien opracować i utrzymywać formalny proces identyfikacji zagrożeń, które mogą mieć wpływ na bezpieczeństwo lotnicze we wszystkich obszarach działania. Dotyczy to sprzętu, urządzeń i systemów. Jakikolwiek zidentyfikowane i kontrolowane zagrożenie związane z bezpieczeństwem lotniczym jest korzystne dla bezpieczeństwa operacji. Ważne jest również rozważenie zagrożeń, które mogą istnieć w wyniku interfejsów SMS z organizacjami zewnętrznymi.

Źródła identyfikacji zagrożeń

9.4.4.1 Istnieje wiele źródeł identyfikacji zagrożeń, wewnętrznych lub zewnętrznych w stosunku do organizacji. Niektóre źródła wewnętrzne obejmują:

- Monitorowanie rutynowych operacji*: wykorzystanie technik obserwacyjnych do monitorowania codziennych operacji i działań, takich jak audyt bezpieczeństwa operacji liniowych (LOSA).
- Zautomatyzowane systemy monitorowania*: wykorzystanie zautomatyzowanych systemów rejestracji do monitorowania parametrów, które mogą być analizowane, takich jak monitorowanie danych lotu (FDM).
- Dobrowolne i obowiązkowe systemy zgłaszania zdarzeń dotyczących bezpieczeństwa*: zapewnienie wszystkim, w tym pracownikom organizacji zewnętrznym, możliwości zgłaszania zagrożeń i innych problemów związanych z bezpieczeństwem organizacji.

- d) *Audyty*: można je wykorzystać do identyfikacji zagrożeń w obrębie audytowanego zadania lub procesu. Powinny one być również skoordynowane ze zmianami organizacyjnymi w celu identyfikacji zagrożeń związanych z wdrożeniem zmiany.
- e) *Informacje zwrotne ze szkoleń*: szkolenie interaktywne (dwukierunkowe) może ułatwić identyfikację nowych zagrożeń przez uczestników.
- f) *Badanie bezpieczeństwa prowadzone przez podmiot lotniczy*: zagrożenia zidentyfikowane w wewnętrznych badaniach bezpieczeństwa i raportach z działań następczych po wypadkach/incydentach.

9.4.4.2 Przykłady zewnętrznych źródeł identyfikacji zagrożeń obejmują:

- a) *Raporty z wypadków lotniczych*: przegląd raportów o wypadkach, może dotyczyć wypadków w tym samym Państwie lub z podobnym typem statku powietrznego, rejonem lub środowiskiem operacyjnym.
- b) *Krajowe obowiązkowe i dobrowolne systemy zgłaszania zdarzeń dotyczących bezpieczeństwa*: niektóre Państwa zapewniają streszczenia zgłoszeń przekazanych przez podmioty lotnicze.
- c) *Audyty nadzoru krajowego i audyty strony trzeciej*: audyty zewnętrzne mogą czasami identyfikować zagrożenia. Mogą one być udokumentowane jako niezidentyfikowane zagrożenie lub ustalone w mniej oczywisty sposób jako ustalenie z audytu.
- d) *Stowarzyszenia handlowe i systemy wymiany informacji*: wiele stowarzyszeń handlowych i grup branżowych może udostępniać dane bezpieczeństwa, które mogą obejmować zidentyfikowane zagrożenia.

System zgłaszania zdarzeń dotyczących bezpieczeństwa

9.4.4.3 Jednym z głównych źródeł identyfikacji zagrożeń jest system zgłaszania zdarzeń dotyczących bezpieczeństwa, zwłaszcza dobrowolny system zgłaszania. Podczas gdy system obowiązkowy jest zwykle stosowany w przypadku incydentów, które miały miejsce, system dobrowolny zapewnia dodatkowy kanał zgłaszania potencjalnych problemów związanych z bezpieczeństwem, takich jak zagrożenia, sytuacje grożące wypadkiem lub błędy. Mogą one dostarczać Państwu i podmiotowi lotniczemu cennych informacji na temat zdarzeń o mniej poważnych skutkach.

9.4.4.4 Ważne jest, aby podmioty lotnicze zapewniały odpowiednią ochronę w celu zachęcenia ludzi do zgłaszania tego, co widzą lub czego doświadczają. Na przykład działania egzekwowania prawa mogą zostać zniesione w przypadku zgłoszeń błędów lub, w pewnych okolicznościach, łamania reguł. Należy wyraźnie stwierdzić, że zgłaszane informacje będą wykorzystywane wyłącznie w celu poprawy bezpieczeństwa. Ma to na celu promowanie skutecznej kultury zgłaszania i proaktywnej identyfikacji potencjalnych niedociągnięć w zakresie bezpieczeństwa.

9.4.4.5 Dobrowolne systemy zgłaszania zdarzeń dotyczących bezpieczeństwa powinny być poufne, wymagając aby wszelkie informacje pozwalające na identyfikację osoby zgłaszającej były znane tylko administratorowi, aby umożliwić podjęcie dalszych działań. Rola administratora powinna być ograniczona do kilku osób, zazwyczaj zastrzeżona dla kierownika ds. bezpieczeństwa i personelu biorącego udział w badaniu. Zachowanie poufności pomoże w ujawnieniu zagrożeń prowadzących do błędu ludzkiego, nie powodując obaw związanych z odwetem lub zażenowaniem. Dobrowolne zgłoszenia zdarzeń dotyczących bezpieczeństwa mogą zostać pozbawione elementów umożliwiających identyfikację i zarchiwizowane po wykonaniu niezbędnych działań następczych. Raporty pozbawione elementów umożliwiających identyfikację mogą być pomocne przy analizie trendów w celu śledzenia skuteczności działań łagodzących ryzyko oraz identyfikacji pojawiających się zagrożeń.

9.4.4.6 Zachęca się personel na wszystkich poziomach i we wszystkich dziedzinach do identyfikowania i zgłaszania zagrożeń i innych problemów związanych z bezpieczeństwem poprzez systemy zgłaszania zdarzeń dotyczących bezpieczeństwa. Aby systemy zgłaszania były skuteczne, powinny być łatwo dostępne dla całego personelu. W zależności od sytuacji, można wykorzystać formularz papierowy, internetowy lub komputerowy. Posiadanie wielu dostępnych metod zgłaszania zwiększa prawdopodobieństwo zaangażowania personelu. Wszyscy powinni być świadomi korzyści płynących ze zgłaszania zdarzeń dotyczących bezpieczeństwa.

9.4.4.7 Każdy, kto złoży zgłoszenie, powinien otrzymać informację zwrotną o tym, jakie decyzje lub działania zostały podjęte. Dostosowanie wymagań systemu zgłaszania, narzędzi i metod analitycznych może ułatwić wymianę informacji dotyczących bezpieczeństwa, a także porównanie niektórych wskaźników poziomu bezpieczeństwa. Informacje zwrotne dla osób składających zgłoszenia w dobrowolnych systemach zgłaszania służą również wykazaniu, że takie zgłoszenia są traktowane poważnie. Pomaga to promować pozytywną kulturę bezpieczeństwa i zachęca do składania zgłoszeń na przyszłość.

9.4.4.8 Może zaistnieć potrzeba filtrowania zgłoszeń na wejściu, kiedy złożona została duża liczba zgłoszeń. Może to oznaczać konieczność przeprowadzenia wstępnej oceny ryzyka bezpieczeństwa mającej ustalić, czy konieczne jest dalsze badanie i jaki jego zakres jest wymagany.

9.4.4.9 Zgłoszenia zdarzeń dotyczących bezpieczeństwa są często filtrowane za pomocą taksonomii lub systemu klasyfikacji. Filtrowanie informacji przy użyciu taksonomii może ułatwić identyfikację wspólnych problemów i trendów. Podmiot lotniczy powinien opracować taksonomie, które odnoszą się do rodzaju prowadzonych przez niego operacji. Wadą stosowania taksonomii jest to, że zidentyfikowane zagrożenie czasami nie pasuje do żadnej ze zdefiniowanych kategorii. Wyzwaniem jest więc użycie taksonomii o odpowiednim stopniu szczegółowości, na tyle konkretnej, że zagrożenia są łatwe do przydzielenia, ale na tyle ogólnej, że zagrożenia są cenne dla analizy. Niektóre Państwa i międzynarodowe stowarzyszenia handlowe opracowały taksonomie, które można zastosować. Rozdział 5 zawiera dodatkowe informacje na temat taksonomii.

9.4.4.10 Inne metody identyfikacji zagrożeń obejmują warsztaty lub spotkania, w których eksperci merytoryczni przeprowadzają szczegółowe scenariusze analizy. Sesje te korzystają ze wsparcia wielu doświadczonych pracowników operacyjnych i technicznych. Obecne posiedzenia komitetów ds. bezpieczeństwa (SRB, SAG, itp.) mogą być wykorzystywane do takich działań, ta sama grupa może być również wykorzystana do oceny powiązanych ryzyk bezpieczeństwa.

9.4.4.11 Zidentyfikowane zagrożenia i ich potencjalne konsekwencje powinny być udokumentowane. Będą one wykorzystywane w procesach oceny ryzyka bezpieczeństwa.

9.4.4.12 Proces identyfikacji zagrożeń uwzględnia wszystkie możliwe zagrożenia, które mogą występować w zakresie działalności podmiotu lotniczego, w tym interfejsy z innymi systemami, zarówno wewnątrz, jak i na zewnątrz organizacji. Po zidentyfikowaniu zagrożeń, należy określić ich konsekwencje (tj. wszelkie określone zdarzenia lub wyniki).

Badanie zagrożeń

9.4.4.13 Identyfikacja zagrożeń powinna mieć charakter ciągły i stanowić część bieżącej działalności podmiotu lotniczego. Niektóre warunki mogą wymagać bardziej szczegółowego badania. Mogą to być:

- a) przypadki, w których organizacja doświadcza niewyjaśnionego wzrostu zdarzeń lotniczych związanych z bezpieczeństwem lub niezgodności z przepisami; lub
- b) istotne zmiany w organizacji lub jej działalności.

9.4.5 Badanie w zakresie bezpieczeństwa wykonywane przez podmiot lotniczy

9.4.5.1 Skuteczne zarządzanie bezpieczeństwem zależy od badań jakości mających na celu analizę zdarzeń i zagrożeń związanych z bezpieczeństwem, a także raportowanie ustaleń i zaleceń w celu poprawy bezpieczeństwa w środowisku operacyjnym.

9.4.5.2 Istnieje wyraźne rozróżnienie pomiędzy badaniem wypadków i incydentów zgodnie z przepisami Załącznika 13 a badaniami w zakresie bezpieczeństwa wykonywanymi przez podmiot lotniczy. Badanie wypadków i poważnych incydentów zgodnie z Załącznikiem 13 leży w gestii Państwa, zgodnie z definicją zawartą w Załączniku 13. Tego typu informacje mają zasadnicze znaczenie dla rozpowszechniania doświadczeń zdobytych w oparciu o wypadki i incydenty. Badanie w zakresie bezpieczeństwa wykonywane przez podmiot lotniczy stanowi element systemu SMS wspierający procesy identyfikacji zagrożeń i oceny ryzyka. Istnieje wiele zdarzeń związanych z bezpieczeństwem, które wykraczają poza Załącznika 13 mogące stanowić cenne źródło identyfikacji zagrożeń lub słabych punktów w środkach kontroli ryzyka. Problemy te mogą zostać ujawnione i usunięte przez badanie w zakresie bezpieczeństwa prowadzone przez podmiot.

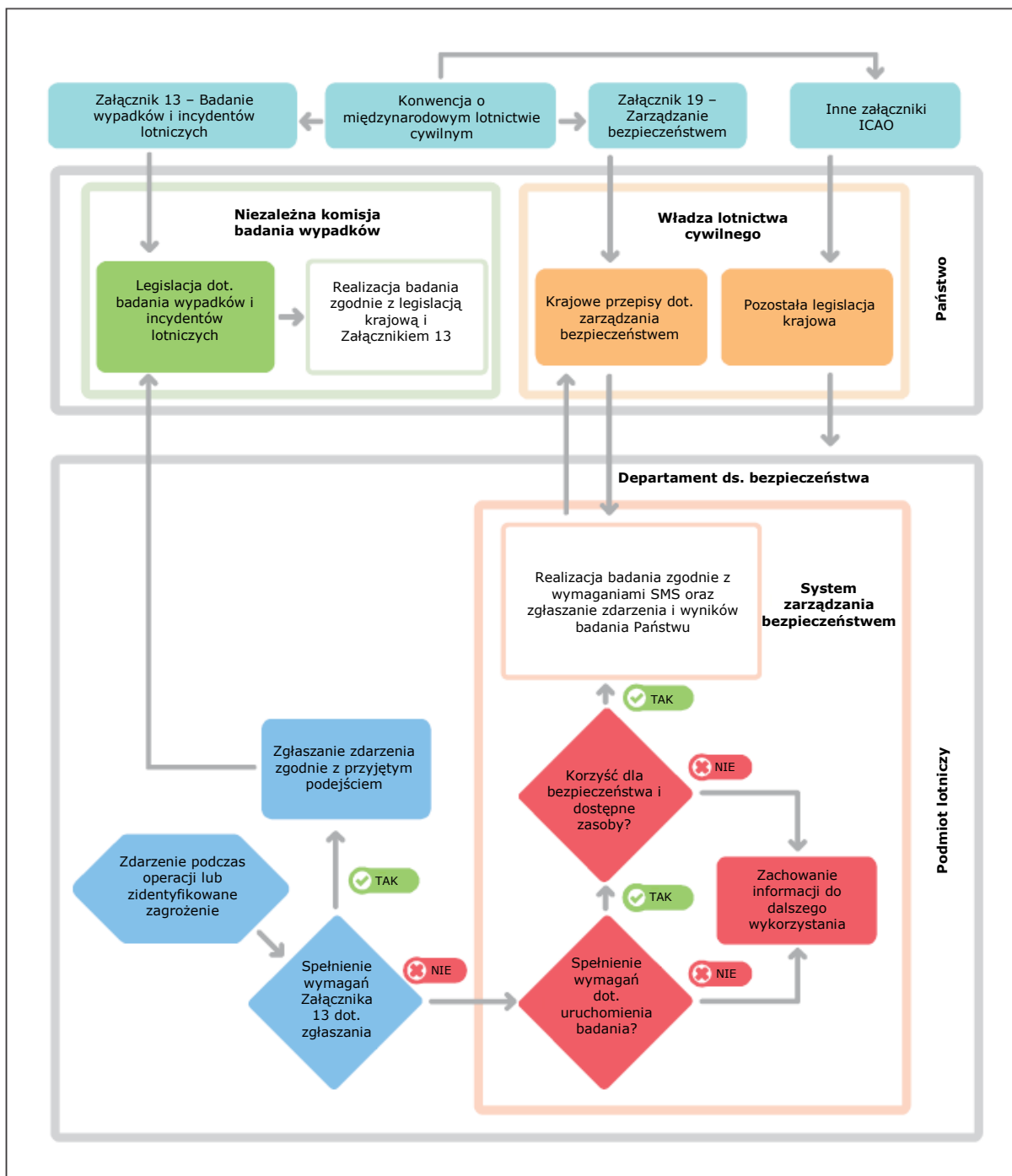
9.4.5.3 Głównym celem badania w zakresie bezpieczeństwa podmiotu lotniczego jest zrozumienie tego, co się stało, oraz zapobieganie występowaniu podobnych sytuacji w przyszłości poprzez eliminowanie lub łagodzenie niedociągnięć w zakresie bezpieczeństwa. Jest to osiągnięte poprzez staranne i metodyczne zbadanie zdarzenia i zastosowanie zdobytych doświadczeń w celu zmniejszenia prawdopodobieństwa i/lub konsekwencji ponownego wystąpienia w przyszłości. Badania w zakresie bezpieczeństwa wykonywane przez podmiot lotniczy stanowią integralną część systemu zarządzania bezpieczeństwem podmiotu.

9.4.5.4 Badania wykonywane przez podmiot lotniczy w zakresie zdarzeń i zagrożeń związanych z bezpieczeństwem stanowią istotne działanie w ramach całego procesu zarządzania ryzykiem w lotnictwie. Korzyści z przeprowadzenia badania w zakresie bezpieczeństwa obejmują:

- a) lepsze zrozumienie wydarzeń prowadzących do zdarzenia;
- b) identyfikowanie sprawczych czynników ludzkich, technicznych i organizacyjnych;
- c) identyfikowanie zagrożeń i przeprowadzanie ocen ryzyka;
- d) wydawanie zaleceń mających na celu zmniejszenie lub wyeliminowanie nieakceptowalnych ryzyk;
oraz
- e) wskazanie zdobytych doświadczeń, którymi należy podzielić się z odpowiednimi członkami społeczności lotniczej.

Czynniki uruchamiające badanie

9.4.5.5 Badanie w zakresie bezpieczeństwa wykonywane przez podmiot lotniczy jest zazwyczaj uruchamiane przez powiadomienie (zgłoszenie) złożone w ramach systemu zgłaszania zdarzeń dotyczących bezpieczeństwa. Rysunek 9-2 przedstawia proces podejmowania decyzji w sprawie badania w zakresie bezpieczeństwa oraz rozróżnienie pomiędzy tym, kiedy powinno mieć miejsce badanie prowadzone przez podmiot, a tym, kiedy powinno być zapoczątkowane badanie zgodnie z przepisami Załącznika 13.



Rysunek 9-2. Proces decyzyjny w badaniu bezpieczeństwa

9.4.5.6 Nie wszystkie zdarzenia lub zagrożenia mogą lub powinny być badane. Decyzja dotycząca przeprowadzenia badania i poziomu jego szczegółowości powinna zależeć od faktycznych lub potencjalnych konsekwencji zdarzenia lub zagrożenia. Istnieje większe prawdopodobieństwo, że zdarzenia i zagrożenia uznawane za posiadające potencjał wysokiego ryzyka będą badane, oraz że badanie to będzie bardziej szczegółowe niż w przypadku zdarzeń i zagrożeń posiadających potencjał niższego ryzyka. Podmioty lotnicze powinny stosować uporządkowane podejście do podejmowania decyzji ze zdefiniowanymi punktami dla czynników uruchamiających. Będą one wpływać na podejmowanie decyzji dotyczących badania w zakresie bezpieczeństwa: co i w jakim zakresie należy zbadać. Dotyczy to:

- a) dotkliwości lub potencjalnej dotkliwości wyniku;

- b) wymagań prawnych lub organizacyjnych dotyczących prowadzenia badania;
- c) wartości bezpieczeństwa, którą należy uzyskać;
- d) możliwości podjęcia działań w zakresie bezpieczeństwa;
- e) ryzyka związanego z brakiem badania;
- f) wkładu w ukierunkowane programy bezpieczeństwa;
- g) zidentyfikowanych trendów;
- h) korzyści szkoleniowych; oraz
- i) dostępności zasobów

Wyznaczenie osoby prowadzącej badanie

9.4.5.7 Jeżeli badanie ma się rozpocząć, pierwszą czynnością będzie wyznaczenie osoby lub, w przypadku dostępności zasobów, zespołu prowadzącego badanie, który dysponuje wymaganymi umiejętnościami i wiedzą. Wielkość zespołu i profil jego członków zależą od charakteru i dotkliwości badanego zdarzenia. Zespół badający może wymagać pomocy ze strony innych specjalistów. Często zdarza się, że jedna osoba jest wyznaczona do przeprowadzenia badania wewnętrznego, przy wsparciu ekspertów ds. operacyjnych i bezpieczeństwa.

9.4.5.8 Najlepiej byłoby, gdyby osoby prowadzące badanie w ramach podmiotu lotniczego były niezależne organizacyjnie od obszaru związanego ze zdarzeniem lub zidentyfikowanym zagrożeniem. Lepsze wyniki zostaną osiągnięte, jeżeli osoba prowadząca badanie jest kompetentna (przeszkolona) i wykwalifikowana (doświadczona) w badaniach bezpieczeństwa prowadzonych przez podmiot. Najlepiej byłoby, gdyby osoby prowadzące badanie były wybierane do tej roli ze względu ich na wiedzę, umiejętności i cechy charakteru, które powinny obejmować: uczciwość, obiektywizm, logiczne myślenie, pragmatyzm i myślenie lateralne.

Proces badania

9.4.5.9 Badanie powinno określić, co się stało i dlaczego tak się stało, a to może wymagać zastosowania analizy przyczyn źródłowych w ramach badania. Najlepiej byłoby, gdyby osoby biorące udział w zdarzeniu były przesłuchiwane jak najszybciej po zdarzeniu. Badanie powinno obejmować:

- a) ustalenie czasu wystąpienia kluczowych zdarzeń, w tym działań zaangażowanych osób;
- b) przegląd wszelkich polityk i procedur związanych z działaniami;
- c) przegląd wszelkich podjętych decyzji związanych ze zdarzeniem;
- d) określenie wszelkich ustanowionych środków kontroli ryzyka, które powinny były zapobiec zdarzeniu; oraz
- e) przegląd danych dotyczących bezpieczeństwa dla poprzednich lub podobnych zdarzeń.

9.4.5.10 Badanie w zakresie bezpieczeństwa powinno koncentrować się na zidentyfikowanych zagrożeniach i ryzykach bezpieczeństwa oraz możliwościach poprawy, a nie na obwinianiu lub karaniu. Sposób prowadzenia badania, a co najważniejsze, sposób w jaki sporządzony zostanie raport, będzie miał wpływ na bezpieczeństwo, przyszłą kulturę bezpieczeństwa organizacji i skuteczność przyszłych inicjatyw w zakresie bezpieczeństwa.

9.4.5.11 Badanie powinno zakończyć się jasno określonymi ustaleniami i zaleceniami, które eliminują lub łagodzą niedociągnięcia w zakresie bezpieczeństwa.

9.4.6 Ocena ryzyka bezpieczeństwa i jego łagodzenie

9.4.6.1 Podmiot lotniczy musi opracować model i procedury oceny ryzyka bezpieczeństwa, które umożliwią spójne i systematyczne podejście do oceny ryzyka bezpieczeństwa. Powinny one określać metodę, która pomoże ustalić, jakie ryzyka bezpieczeństwa są akceptowalne lub nieakceptowalne oraz ustalić priorytety działań.

9.4.6.2 Użyte narzędzia SRM mogą wymagać okresowego przeglądu i dostosowania, aby upewnić się, że są odpowiednie dla środowiska operacyjnego podmiotu lotniczego. Podmiot ten może znaleźć bardziej zaawansowane podejścia, które lepiej odzwierciedlają potrzeby w zakresie działania, w miarę rozwoju systemu SMS. Podmiot lotniczy oraz władza lotnictwa cywilnego powinni uzgodnić metodologię.

9.4.6.3 Dostępne są bardziej zaawansowane podejścia do klasyfikacji ryzyka bezpieczeństwa. Mogą one być bardziej odpowiednie, jeżeli podmiot lotniczy posiada doświadczenie w zarządzaniu bezpieczeństwem lub w działaniu w środowisku wysokiego ryzyka.

9.4.6.4 W procesie oceny ryzyka bezpieczeństwa należy wykorzystywać wszelkie dane bezpieczeństwa i informacje bezpieczeństwa. Po dokonaniu oceny ryzyka, podmiot lotniczy zaangażuje się w proces podejmowania decyzji w oparciu o dane w celu określenia niezbędnych środków kontroli ryzyka bezpieczeństwa.

9.4.6.5 Oceny ryzyka bezpieczeństwa muszą czasami bazować na informacjach jakościowych (osąd ekspercki), a nie na danych ilościowych z powodu ich niedostępności. Stosowanie matrycy ryzyka bezpieczeństwa pozwala użytkownikowi wyrazić ryzyko bezpieczeństwa związane ze zidentyfikowanym zagrożeniem w formacie ilościowym. Umożliwia to bezpośrednie porównanie wielkości zidentyfikowanych ryzyk bezpieczeństwa. Możliwe jest zastosowanie jakościowego kryterium oceny ryzyka bezpieczeństwa, takiego jak „prawdopodobne wystąpienie” lub „nieprawdopodobne” przypisane do każdego zidentyfikowanego ryzyka, w sytuacji gdy dane ilościowe nie są dostępne.

9.4.6.6 W przypadku podmiotów lotniczych w wielu lokalizacjach o określonych środowiskach operacyjnych, bardziej efektywne może być ustanowienie lokalnych komitetów ds. bezpieczeństwa w celu przeprowadzenia oceny ryzyka bezpieczeństwa i określenia środków kontroli ryzyka bezpieczeństwa. Częstym przypadkiem jest poszukiwanie porady wśród specjalistów z obszaru operacyjnego (wewnątrz lub na zewnątrz podmiotu lotniczego). Ostateczne decyzje lub akceptacja środków kontroli może być wymagana od władz wyższego szczebla w celu zapewnienia odpowiednich zasobów.

9.4.6.7 Sposób, w jaki podmioty lotnicze ustalają priorytety ocen ryzyka bezpieczeństwa i przyjmują środki kontroli ryzyka bezpieczeństwa, stanowi ich decyzję. Jako wytyczne do wykorzystania w procesie ustalania priorytetów, podmiot powinien przyjąć że proces ten uwzględnia:

- a) ocenę i kontrolę najwyższego ryzyka bezpieczeństwa;
- b) alokację zasobów dla najwyższego ryzyka bezpieczeństwa;
- c) skuteczne utrzymanie lub poprawę bezpieczeństwa;
- d) osiągnięcie określonych i uzgodnionych celów bezpieczeństwa i SPT; oraz
- e) spełnienie wymagań przepisów krajowych w zakresie kontroli ryzyka bezpieczeństwa.

9.4.6.8 Po przeprowadzeniu oceny ryzyka bezpieczeństwa, można wdrożyć odpowiednie środki kontroli ryzyka bezpieczeństwa. Ważne jest, aby w określanie odpowiednich środków kontroli ryzyka zaangażować „użytkowników końcowych” i ekspertów z danej dziedziny. Zapewnienie zaangażowania właściwych osób pozwoli zwiększyć praktyczność wybranych działań łagodzących. Określenie wszelkich niezamierzonych konsekwencji, w szczególności wprowadzenie nowych zagrożeń, powinno być dokonane przed wdrożeniem jakichkolwiek środków kontroli ryzyka bezpieczeństwa.

9.4.6.9 Po uzgodnieniu i wdrożeniu środków kontroli ryzyka bezpieczeństwa, poziom bezpieczeństwa powinien być monitorowany w celu zapewnienia skuteczności środków kontroli ryzyka bezpieczeństwa. Jest to konieczne, aby zweryfikować integralność, wydajność i skuteczność nowych środków kontroli ryzyka w warunkach operacyjnych.

9.4.6.10 Dane wyjściowe w procesie zarządzania ryzykiem bezpieczeństwa powinny być udokumentowane. Dotyczy to zagrożenia i wszelkich konsekwencji, oceny ryzyka bezpieczeństwa i wszelkich podejmowanych działań związanych z kontrolą ryzyka bezpieczeństwa. Dane są one często zapisywane w rejestrze, dzięki czemu można je śledzić i monitorować. Ta dokumentacja SRM staje się historycznym źródłem wiedzy o bezpieczeństwie organizacji, która może być wykorzystana jako odniesienie przy podejmowaniu decyzji dotyczących bezpieczeństwa oraz do wymiany informacji dotyczących bezpieczeństwa. Wiedza na temat bezpieczeństwa stanowi materiał do analiz trendów bezpieczeństwa oraz szkoleń i komunikacji w zakresie bezpieczeństwa. Jest ona również przydatna w prowadzeniu audytów wewnętrznych przy ocenie czy środki kontroli i działania w zakresie ryzyka bezpieczeństwa zostały wdrożone i są skuteczne.

9.5. KOMPONENT NR 3: ZAPEWNIANIE BEZPIECZEŃSTWA

9.5.1 Załącznik 19, Dodatek 2, pkt 3.1.1 wymaga, aby podmioty lotnicze opracowały i utrzymywały środki pozwalające na zweryfikowanie poziomu bezpieczeństwa organizacji i sprawdzenie skuteczności kontroli ryzyka bezpieczeństwa. Komponent zapewniania bezpieczeństwa systemu zarządzania bezpieczeństwem podmiotu zapewnia te możliwości.

9.5.2 Zapewnianie bezpieczeństwa składa się z procesów i działań podejmowanych w celu ustalenia, czy system SMS działa zgodnie z oczekiwaniami i wymaganiami. Wiąże się to z ciągłym monitorowaniem jego procesów oraz środowiska operacyjnego w celu wykrycia zmian lub odchyień, które mogą powodować pojawienie się nowych ryzyk bezpieczeństwa lub pogorszenie działania istniejących środków kontroli ryzyka bezpieczeństwa. Takie zmiany lub odchylenia można następnie rozwiązać za pomocą procesu SRM.

9.5.3 Działania związane z zapewnianiem bezpieczeństwa powinny obejmować opracowywanie i wdrażanie działań podjętych w odpowiedzi na wszelkie zidentyfikowane problemy mające potencjalny wpływ na bezpieczeństwo. Działania te stale poprawiają wydajność systemu zarządzania bezpieczeństwem podmiotu lotniczego.

9.5.4 Monitorowanie i pomiar poziomu bezpieczeństwa

Weryfikacja poziomu bezpieczeństwa organizacji i sprawdzenie skuteczności kontroli ryzyka bezpieczeństwa wymaga zastosowania połączenia audytów wewnętrznych oraz ustanowienia i monitorowania SPI. Ocena skuteczności środków kontroli ryzyka bezpieczeństwa jest ważna, ponieważ ich zastosowanie nie zawsze pozwala osiągnąć zamierzone rezultaty. Pomoże to określić, czy wybrano właściwy środek kontroli ryzyka bezpieczeństwa i może skutkować zastosowaniem innej strategii kontroli ryzyka bezpieczeństwa.

Audyt wewnętrzny

9.5.4.1 Audyty wewnętrzne są przeprowadzane w celu oceny skuteczności systemu SMS oraz określenia obszarów potencjalnej poprawy. Większość przepisów bezpieczeństwa lotniczego dotyczy ogólnych środków kontroli ryzyka bezpieczeństwa, które zostały ustanowione przez Państwo. Zapewnienie zgodności z przepisami poprzez audyt wewnętrzny jest podstawowym aspektem zapewniania bezpieczeństwa.

9.5.4.2 Konieczne jest również zapewnienie skutecznego wdrożenia i monitorowania wszelkich środków kontroli ryzyka bezpieczeństwa. Przyczyny i czynniki sprawcze powinny zostać zbadane i przeanalizowane w przypadku zidentyfikowania niezgodności i innych problemów. Audyt wewnętrzny koncentruje się przede wszystkim na politykach, procesach i procedurach zapewniających środki kontroli ryzyka bezpieczeństwa.

9.5.4.3 Audyty wewnętrzne są najskuteczniejsze, kiedy są przeprowadzane przez osoby lub działy niezależne od kontrolowanych funkcji. Takie audyty powinny zapewniać dyrektorowi odpowiedzialnemu i kierownictwu wyższego szczebla informacje zwrotne na temat:

- a) zgodności z przepisami;
- b) zgodności z politykami, procesami i procedurami;
- c) skuteczności środków kontroli ryzyka bezpieczeństwa;
- d) skuteczności działań naprawczych; oraz
- e) skuteczności systemu SMS.

9.5.4.4 Niektóre organizacje nie mogą zapewnić odpowiedniej niezależności audytu wewnętrznego, w takich przypadkach podmiot lotniczy powinien rozważyć zaangażowanie audytorów zewnętrznych (np. niezależnych audytorów lub audytorów z innej organizacji).

9.5.4.5 Planowanie audytów wewnętrznych powinno uwzględniać krytyczność procesów dla bezpieczeństwa, wyniki poprzednich audytów i ocen (ze wszystkich źródeł) oraz wdrożone środki kontroli ryzyka bezpieczeństwa. Audyty wewnętrzne powinny identyfikować niezgodność z przepisami i politykami, procesami i procedurami. Powinny także identyfikować niedociągnięcia systemu, brak skuteczności środków kontroli ryzyka bezpieczeństwa oraz możliwości poprawy.

9.5.4.6 Ocena zgodności i skuteczności ma zasadnicze znaczenie w osiągnięciu poziomu bezpieczeństwa. Proces audytu wewnętrznego można wykorzystać do określenia zarówno zgodności, jak i skuteczności. W celu oceny zgodności i skuteczności każdego procesu lub procedury można zadać następujące pytania:

- a) Określenie zgodności
 - 1) Czy istnieje wymagany proces lub procedura?
 - 2) Czy proces lub procedura są udokumentowane (zdefiniowane dane wejściowe, działania, interfejsy i dane wyjściowe)?
 - 3) Czy proces lub procedura spełniają wymagania (kryteria)?
 - 4) Czy proces lub procedura są używane?
 - 5) Czy cały zaangażowany personel konsekwentnie realizuje proces lub procedurę?
 - 6) Czy zdefiniowane dane wyjściowe są generowane?
 - 7) Czy zmiana procesu lub procedury została udokumentowana i wdrożona?
- b) Ocena skuteczności
 - 1) Czy użytkownicy rozumieją proces lub procedurę?
 - 2) Czy cel procesu lub procedury jest konsekwentnie osiągany?
 - 3) Czy wyniki procesu lub procedury są tym, czego życzył sobie „klient”?
 - 4) Czy proces lub procedura są regularnie poddawane przeglądom?
 - 5) Czy przeprowadzana jest ocena ryzyka bezpieczeństwa w przypadku zmian w procesie lub procedurze?

6) Czy usprawnienia procesów lub procedur przyniosły oczekiwane korzyści?

9.5.4.7 Ponadto, audyty wewnętrzne powinny monitorować postępy w zamykaniu wcześniej zidentyfikowanych niezgodności. Powinny one zostać rozwiązane poprzez analizę przyczyn źródłowych oraz opracowanie i wdrożenie planów działań naprawczych i zapobiegawczych. Wyniki analizy przyczyn i czynników sprawczych wszelkich niezgodności powinny zasilać procesy zarządzania ryzykiem bezpieczeństwa (SRM) podmiotu lotniczego.

9.5.4.8 Wyniki procesu audytu wewnętrznego stają się danymi wejściowymi w procesie SRM lub zapewniania bezpieczeństwa. Audyty wewnętrzne stanowią źródło informacji dla kierownictwa podmiotu lotniczego na temat poziomu zgodności organizacji, stopnia, w jakim środki kontroli ryzyka bezpieczeństwa są skuteczne oraz obszarów gdzie wymagane są działania naprawcze lub zapobiegawcze.

9.5.4.9 Władze lotnictwa cywilnego mogą zapewnić dodatkowe informacje zwrotne na temat statusu zgodności z przepisami i skuteczności systemu SMS oraz stowarzyszenia branżowe lub inne strony trzecie wybrane przez podmiot lotniczy do prowadzenia audytu organizacji i procesów. Wyniki takich audytów przeprowadzanych przez drugą i trzecią stronę stanowią dane wejściowe do funkcji zapewniania bezpieczeństwa, dostarczając podmiotowi lotniczemu wskazań co do skuteczności ich procesów audytu wewnętrznego i możliwości poprawy systemu SMS.

Monitorowanie poziomu bezpieczeństwa

9.5.4.10 Monitorowanie poziomu bezpieczeństwa jest realizowane poprzez gromadzenie danych bezpieczeństwa i informacji bezpieczeństwa z różnych źródeł, które są zazwyczaj dostępne dla organizacji. Dostępność danych wspierających świadome podejmowanie decyzji jest jednym z najważniejszych aspektów systemu SMS. Wykorzystanie tych danych do monitorowania i pomiaru poziomu bezpieczeństwa stanowi zasadnicze działania, które generują informacje niezbędne do podejmowania decyzji dotyczących ryzyka bezpieczeństwa.

9.5.4.11 Monitorowanie i pomiar poziomu bezpieczeństwa powinny być przeprowadzane z zachowaniem pewnych podstawowych zasad. Osiągnięty poziom bezpieczeństwa stanowi wskaźnik zachowania organizacji i jest również miarą skuteczności systemu zarządzania bezpieczeństwem. Wymaga to od organizacji zdefiniowania:

- a) celów bezpieczeństwa, które powinny zostać ustanowione w pierwszej kolejności w celu odzwierciedlenia strategicznych osiągnięć lub pożądanych wyników związanych z obawami dotyczącymi bezpieczeństwa specyficznymi dla kontekstu operacyjnego organizacji;
- b) SPI, które są parametrami taktycznymi związanymi z celami bezpieczeństwa i dlatego stanowią odniesienie do zbierania danych; oraz
- c) SPT, które są również parametrami taktycznymi służącymi do monitorowania postępów w osiąganiu celów bezpieczeństwa.

9.5.4.12 Bardziej kompletny i realistyczny obraz poziomu bezpieczeństwa podmiotu lotniczego zostanie osiągnięty, jeżeli SPI obejmują szerokie spektrum wskaźników. Dotyczy to:

- a) wydarzeń o małym prawdopodobieństwie/dużej dotkliwości (np. wypadki i poważne incydenty);
- b) wydarzeń o dużym prawdopodobieństwie/malej dotkliwości (np. niepomyślne zdarzenia operacyjne, raporty niezgodności, odchylenia, itp.); oraz
- c) działania procesu (np. szkolenia, ulepszenia systemu i przetwarzanie zgłoszeń).

9.5.4.13 SPI są używane do pomiaru poziomu bezpieczeństwa operacyjnego i działania systemu SMS podmiotu lotniczego. SPI polegają na monitorowaniu danych i informacji z różnych źródeł, w tym na systemie zgłaszania zdarzeń dotyczących bezpieczeństwa. SPI powinny być specyficzne dla poszczególnych podmiotów i powiązane z ustanowionymi celami bezpieczeństwa.

9.5.4.14 Podczas ustanawiania SPI podmioty prowadzące działalność w lotnictwie cywilnym powinny rozważyć:

- a) *Pomiar właściwych parametrów*: Należy określić najlepsze SPI, które pokażą, że organizacja jest na dobrej drodze do osiągnięcia celów bezpieczeństwa. Należy się również zastanowić, jakie są największe problemy związane z bezpieczeństwem i ryzyka bezpieczeństwa, w obliczu których stoi organizacja, oraz zidentyfikować SPI, które pokażą skuteczną kontrolę nad nimi.
- b) *Dostępność danych*: Czy dostępne są dane, które są zgodne z tym, co organizacja chce zmierzyć? Jeżeli nie, może zaistnieć potrzeba ustanowienia dodatkowych źródeł gromadzenia danych. W przypadku małych organizacji z ograniczoną ilością danych, gromadzenie zbiorów danych może również pomóc w identyfikacji trendów. Może to być wspierane przez stowarzyszenia branżowe, które mogą zestawiać dane bezpieczeństwa z wielu organizacji.
- c) *Wiarygodność danych*: Dane mogą być niewiarygodne ze względu na ich subiektywność lub niekompletność.
- d) *Wspólne branżowe SPI*: Przydatne może być uzgodnienie wspólnych SPI z podobnymi organizacjami, aby można było dokonać porównań pomiędzy organizacjami. Organ regulacyjny i stowarzyszenia branżowe mogą to umożliwić.

9.5.4.15 Po ustanowieniu SPI podmiot lotniczy powinien rozważyć, czy wskazane jest określenie SPT i poziomów alarmowych. SPT są przydatne w poprawie bezpieczeństwa, ale jeżeli są źle wdrażane, mogą prowadzić do niepożądanych zachowań – co w praktyce polega na tym, że jednostki i działy koncentrują się w zbyt dużym stopniu na osiągnięciu celu, tracąc z pola widzenia to, co sam cel miał osiągnąć – zamiast poprawić poziom bezpieczeństwa organizacji. W takich przypadkach bardziej odpowiednie może być monitorowanie SPI pod kątem trendów.

9.5.4.16 Poniższe działania mogą zapewnić źródła dla monitorowania i pomiaru poziomu bezpieczeństwa:

- a) *Studia bezpieczeństwa* to analizy mające na celu głębsze zrozumienie problemów związanych z bezpieczeństwem lub lepsze zrozumienie trendów w zakresie bezpieczeństwa.
- b) *Analiza danych dotyczących bezpieczeństwa* wykorzystuje dane ze zgłoszeń zdarzeń dotyczących bezpieczeństwa w celu wykrycia wspólnych problemów lub trendów, które mogą uzasadniać dalsze badanie.
- c) *Przeglądy bezpieczeństwa* badają procedury lub procesy związane z konkretną operacją. Przeglądy bezpieczeństwa mogą obejmować zastosowanie list kontrolnych, kwestionariuszy oraz nieformalne poufne rozmowy. Przeglądy bezpieczeństwa zazwyczaj dostarczają informacji jakościowych. Mogą one wymagać weryfikacji poprzez zbieranie danych w celu ustalenia, czy wymagane są działania naprawcze. Niemniej jednak przeglądy mogą stanowić niedrogie i wartościowe źródło informacji dotyczących bezpieczeństwa.
- d) *Audyty bezpieczeństwa* skupiają się na ocenie integralności systemu SMS i systemów zabezpieczających podmiotu lotniczego. Audyty bezpieczeństwa mogą być również wykorzystywane do oceny skuteczności wdrożonych środków kontroli ryzyka bezpieczeństwa lub monitorowania zgodności z przepisami bezpieczeństwa. Zapewnienie niezależności i obiektywizmu stanowi wyzwanie dla audytów bezpieczeństwa. Niezależność i obiektywizm można osiągnąć angażując

zewnętrzne podmioty lub audyty wewnętrzne z obowiązującymi zabezpieczeniami w postaci polityk, procedur, protokołów dotyczących komunikacji.

- e) *Ustalenia i zalecenia z badań w zakresie bezpieczeństwa* mogą dostarczyć użytecznych informacji dotyczących bezpieczeństwa, które można przeanalizować w odniesieniu do innych zebranych danych dotyczących bezpieczeństwa.
- f) *Systemy gromadzenia danych operacyjnych*, takie jak FDA, informacje radarowe mogą dostarczyć użytecznych danych o zdarzeniach i wydajności operacyjnej.

9.5.4.17 Opracowanie SPI powinno być powiązane z celami bezpieczeństwa i opierać się na analizie danych, które są dostępne lub możliwe do uzyskania. Proces monitorowania i pomiaru obejmuje wykorzystanie wybranych wskaźników poziomu bezpieczeństwa, odpowiednich SPT i czynników uruchamiających.

9.5.4.18 Organizacja powinna monitorować działanie ustanowionych SPI i SPT w celu identyfikacji anormalnych zmian w poziomie bezpieczeństwa. SPT powinny być realistyczne, specyficzne dla kontekstu i osiągalne przy uwzględnieniu zasobów dostępnych dla organizacji i powiązanego sektora lotniczego.

9.5.4.19 Przede wszystkim, monitorowanie i pomiar poziomu bezpieczeństwa zapewniają środki do weryfikacji skuteczności kontroli ryzyka bezpieczeństwa. Ponadto, zapewniają miarę integralności i skuteczności procesów i działań systemu SMS.

9.5.4.20 Państwo może posiadać określone procesy akceptacji SPI i SPT, których należy przestrzegać. Dlatego podczas opracowywania SPI i SPT, podmiot lotniczy powinien konsultować się z właściwym organem regulacyjnym lub stosować się do wszelkich powiązanych informacji opublikowanych przez Państwo.

9.5.4.21 Więcej informacji na temat zarządzania poziomem bezpieczeństwa znajduje się w Rozdziale 4.

9.5.5 Zarządzanie zmianą

9.5.5.1 Podmioty lotnicze doświadczają zmian ze względu na wiele czynników, w tym między innymi:

- a) ekspansja lub kurczenie się organizacji;
- b) usprawnienia biznesowe wpływające na bezpieczeństwo; mogą one powodować zmiany w systemach wewnętrznych, procesach lub procedurach, które stanowią wsparcie w bezpiecznym zapewnianiu produktów i usług;
- c) zmiany w środowisku operacyjnym organizacji;
- d) zmiany interfejsów SMS z organizacjami zewnętrznymi; oraz
- e) zewnętrzne zmiany prawne, zmiany gospodarcze i pojawiające się ryzyka.

9.5.5.2 Zmiana może mieć wpływ na skuteczność istniejących środków kontroli ryzyka bezpieczeństwa. Ponadto nowe zagrożenia i związane z nimi ryzyka bezpieczeństwa mogą zostać przypadkowo wprowadzone, gdy ma miejsce zmiana. Zagrożenia powinny być identyfikowane, a związane z nimi ryzyka bezpieczeństwa powinny być oceniane i kontrolowane zgodnie z istniejącymi procedurami identyfikacji zagrożeń lub zarządzania ryzykiem bezpieczeństwa organizacji.

9.5.5.3 Proces zarządzania zmianą w organizacji powinien uwzględniać następujące kwestie:

- a) Krytyczność. Jak krytyczna jest zmiana? Podmiot lotniczy powinien uwzględnić wpływ na działania organizacji oraz wpływ na inne organizacje i system lotniczy.

- b) Dostępność ekspertów w danej dziedzinie. Ważne jest, aby kluczowi członkowie społeczności lotniczej byli zaangażowani w działania związane z zarządzaniem zmianą. Może to dotyczyć osób z organizacji zewnętrznych.
- c) Dostępność danych i informacji dotyczących poziomu bezpieczeństwa. Jakie dane i informacje są dostępne, które można wykorzystać do przekazania informacji o sytuacji i umożliwienia analizy zmiany?

9.5.5.4 Małe zmiany często pozostają niezauważone, ale łączny efekt może być znaczny. Zmiany duże i małe mogą mieć wpływ na opis systemu organizacji i mogą powodować konieczność jego zmiany. Dlatego opis systemu powinien być poddawany regularnym przeglądom w celu określenia jego ciągłej aktualności, mając na uwadze, że większość podmiotów lotniczych doświadcza regularnych, a nawet ciągłych zmian.

9.5.5.5 Podmiot lotniczy powinien zdefiniować czynnik uruchamiający formalny proces zmiany. Zmiany, które mogą uruchomić formalne zarządzanie zmianą, obejmują:

- a) wprowadzenie nowych technologii lub sprzętu;
- b) zmiany w środowisku operacyjnym;
- c) zmiany w kluczowym personelu;
- d) znaczące zmiany poziomu zatrudnienia;
- e) zmiany w przepisach dotyczących bezpieczeństwa;
- f) znacząca restrukturyzacja organizacji; oraz
- g) zmiany fizyczne (nowy obiekt lub baza, zmiany układu lotniska, itp.).

9.5.5.6 Podmiot lotniczy powinien również uwzględnić wpływ zmiany na personel. Może to wpłynąć na sposób, w jaki zmiana jest akceptowana przez osoby, których dotyczy. Komunikacja i zaangażowanie na wczesnym etapie poprawią sposób postrzegania i wdrażania zmiany.

9.5.5.7 Proces zarządzania zmianą powinien obejmować następujące działania:

- a) *zrozumienie i zdefiniowanie zmiany*: należy opracować opis zmiany wraz z przyczynami jej wdrażania;
- b) *zrozumienie i zdefiniowanie, na kogo i na co zmiana wpłynie*: mogą to być osoby w organizacji, inne departamenty, osoby lub organizacje zewnętrzne. Mogą to być również urządzenia, systemy i procesy, na które zmiana będzie mieć wpływ. Potrzebny może okazać się przegląd opisu systemu i interfejsów organizacji. Jest to etap, na którym można określić, kto powinien być zaangażowany w zmianę. Zmiany mogą wpłynąć na ustanowione środki kontroli ryzyka mające łagodzić inne ryzyka, a zatem zmiany mogą zwiększyć ryzyko w obszarach, które nie od razu są oczywiste;
- c) *zidentyfikowanie zagrożeń związanych ze zmianą i przeprowadzenie oceny ryzyka bezpieczeństwa*: należy zidentyfikować wszystkie zagrożenia bezpośrednio związane ze zmianą. Wpływ na istniejące zagrożenia i środki kontroli ryzyka bezpieczeństwa, na które zmiana może wpływać, należy również podlegać przeglądowi. Na tym etapie należy wykorzystać istniejące procesy SRM organizacji;
- d) *opracowanie planu działania*: plan powinien określać, co należy zrobić, kto i kiedy powinien to zrobić. Plan powinien jednoznacznie określać sposób wdrożenia zmiany i jednostkę odpowiedzialną za wszystkie działania, oraz kolejność i harmonogram każdego zadania;

- e) *podpisanie się pod zmianą*: ma to na celu potwierdzenie, że zmiana jest bezpieczna do wdrożenia. Osoba, której powierzono obowiązek i uprawnienia do wdrożenia zmiany, powinna podpisać plan wdrożenia zmiany; oraz
- f) *plan ubezpieczenia*: ma on na celu określenie koniecznych działań następczych. Należy rozważyć sposób, w jaki informacje o zmianie zostaną rozpowszechnione oraz czy wymagane są dodatkowe działania (takie jak audyty) w trakcie lub po wdrożeniu zmiany. Wszelkie przyjęte założenia należy przetestować.

9.5.6 Ciągłe doskonalenie systemu zarządzania bezpieczeństwem

9.5.6.1 Załącznik 19, Dodatek 2, pkt 3.3 określa, że ... „podmiot lotniczy monitoruje i ocenia procesy SMS w celu utrzymania lub ciągłej poprawy ogólnej skuteczności SMS”. Utrzymanie i ciągłe doskonalenie skuteczności SMS podmiotu lotniczego jest wspierane przez działania związane z zapewnianiem bezpieczeństwa, które obejmują weryfikację i monitorowanie działań oraz procesów audytu wewnętrznego. Należy uznać, że utrzymanie i ciągłe doskonalenie SMS są jak niekończąca się podróż, ponieważ sama organizacja i środowisko operacyjne będą się nieustannie zmieniać.

9.5.6.2 Audyty wewnętrzne polegają na ocenie działań podmiotu lotniczego, która może dostarczyć informacji przydatnych w procesach decyzyjnych organizacji. Funkcja audytu wewnętrznego obejmuje ocenę wszystkich funkcji zarządzania bezpieczeństwem w całej organizacji.

9.5.6.3 Skuteczność SMS nie powinna opierać się wyłącznie na SPI. Podmioty lotnicze powinny dążyć do wdrożenia zróżnicowanych metod określania jego skuteczności, pomiaru danych wyjściowych oraz wyników procesów, a także oceny informacji zebranych w ramach tych działań. Metody takie mogą obejmować:

- a) *Audyty*: obejmują audyty wewnętrzne i audyty przeprowadzane przez inne organizacje.
- b) *Oceny*: obejmują oceny kultury bezpieczeństwa i skuteczności SMS.
- c) *Monitorowanie zdarzeń*: monitorowanie powtarzających się zdarzeń dotyczących bezpieczeństwa, w tym wypadków i incydentów jak również błędów i sytuacji łamania reguł.
- d) *Przeglądy bezpieczeństwa*: w tym przeglądy kulturowe zapewniające przydatne informacje zwrotne na temat zaangażowania pracowników w SMS. Mogą również stanowić wskaźnik kultury bezpieczeństwa organizacji.
- e) *Przeglądy realizowane przez kierownictwo*: przeglądy te polegają na sprawdzeniu, czy organizacja osiąga ustanowione cele bezpieczeństwa oraz stanowią okazję do przyjrzenia się wszystkim dostępnym informacjom dotyczącym poziomu bezpieczeństwa w celu identyfikacji ogólnych trendów. Ważne jest, aby kierownictwo wyższego szczebla prowadziło przegląd skuteczności SMS. Może to być realizowane jako jedna z funkcji komitetu ds. bezpieczeństwa najwyższego szczebla.
- f) *Ocena SPI i SPT*: możliwa w ramach przeglądu realizowanego przez kierownictwo. Uwzględnia trendy oraz, w przypadku dostępności odpowiednich danych, można je porównać z danymi innych podmiotów lotniczych lub Państw lub na poziomie globalnym.
- g) *Uwzględnienie zdobytych doświadczeń*: w oparciu o systemy zgłaszania zdarzeń dotyczących bezpieczeństwa oraz badania w zakresie bezpieczeństwa wykonywane przez podmioty lotnicze. Powinny one prowadzić do poprawy bezpieczeństwa.

9.5.6.4 Podsumowując, monitorowanie poziomu bezpieczeństwa i procesów audytu wewnętrznego przyczynia się do zdolności podmiotu lotniczego do ciągłej poprawy poziomu bezpieczeństwa. Bieżące monitorowanie systemu SMS, związane z nimi środki kontroli ryzyka bezpieczeństwa i systemy zabezpieczające

zapewniają podmiot i Państwo, że procesy zarządzania bezpieczeństwem osiągają pożądane cele w zakresie poziomu bezpieczeństwa.

9.6. KOMPONENT NR 4: PROMOWANIE BEZPIECZEŃSTWA

9.6.1 Promowanie bezpieczeństwa zachęca do pozytywnej kultury bezpieczeństwa i pomaga osiągnąć cele bezpieczeństwa podmiotu lotniczego poprzez połączenie kompetencji technicznych, które są stale poprawiane poprzez szkolenie i kształcenie, skutecznej komunikacji i udostępniania informacji. Kierownictwo wyższego szczebla zapewnia przywództwo w promowaniu kultury bezpieczeństwa w całej organizacji.

9.6.2 Skuteczne zarządzanie bezpieczeństwem nie może być osiągnięte wyłącznie poprzez mandat lub ściśle przestrzeganie polityk i procedur. Promowanie bezpieczeństwa wpływa zarówno na zachowania indywidualne, jak i organizacyjne, i stanowi uzupełnienie polityk, procedur i procesów organizacji, zapewniając system wartości wspierający wysiłki w zakresie bezpieczeństwa.

9.6.3 Podmiot lotniczy powinien ustanowić i wdrożyć procesy i procedury ułatwiające skuteczną dwustronną komunikację na wszystkich szczeblach organizacji. Powinny one wskazywać wyraźny kierunek strategiczny począwszy od kierownictwa organizacji i umożliwiać „oddolną” komunikację, która zachęca do przekazywania konstruktywnych informacji zwrotnych przez cały personel.

9.6.4 Szkolenie i kształcenie

9.6.4.1 Załącznik 19 określa, że „podmiot lotniczy opracowuje i utrzymuje program szkolenia w zakresie bezpieczeństwa, który zapewnia, że personel jest przeszkolony i kompetentny do wykonywania obowiązków SMS”. Określa również, że „zakres programu szkolenia w zakresie bezpieczeństwa jest odpowiedni do zaangażowania każdej osoby w SMS.” Kierownik ds. bezpieczeństwa jest odpowiedzialny za zapewnienie odpowiedniego programu szkolenia w zakresie bezpieczeństwa. Wiąże się to z dostarczeniem odpowiednich informacji bezpieczeństwa istotnych dla konkretnych problemów związanych z bezpieczeństwem, na jakie napotyka organizacja. Personel, który jest przeszkolony i kompetentny do wykonywania swoich obowiązków SMS, niezależnie od szczebla organizacji, jest wyznacznikiem zaangażowania kierownictwa w skuteczny SMS. Program szkolenia powinien obejmować wymagania w zakresie szkolenia wstępnego i okresowego w celu utrzymania kompetencji. Szkolenie wstępne w zakresie bezpieczeństwa powinno uwzględniać co najmniej następujące zagadnienia:

- a) polityki bezpieczeństwa i cele bezpieczeństwa organizacji;
- b) role i obowiązki organizacji w zakresie bezpieczeństwa;
- c) podstawowe zasady SRM;
- d) systemy zgłaszania zdarzeń dotyczących bezpieczeństwa;
- e) procesy i procedury SMS organizacji; oraz
- f) czynniki ludzkie.

9.6.4.2 Szkolenie okresowe w zakresie bezpieczeństwa powinno skupiać się na zmianach w politykach, procesach i procedurach SMS oraz powinno podkreślać wszelkie szczególne problemy związane z bezpieczeństwem istotne dla organizacji lub zdobyte doświadczenia.

9.6.4.3 Program szkolenia powinien być dostosowany do potrzeb danej osoby i funkcji realizowanej w ramach SMS. Na przykład, zakres i poziom szczegółowości szkolenia dla kierowników zaangażowanych w komitety ds. bezpieczeństwa organizacji będzie większy niż w przypadku personelu bezpośrednio zaangażowanego w

zapewnianie produktu lub usług organizacji. Personel, który nie jest bezpośrednio zaangażowany w operacje, może wymagać jedynie ogólnego przeglądu systemu SMS organizacji.

Analiza potrzeb szkoleniowych

9.6.4.4 W przypadku większości organizacji, konieczne jest przeprowadzenie formalnej analizy potrzeb szkoleniowych (TNA) w celu zapewnienia jednoznacznego zrozumienia działań, obowiązków personelu w zakresie bezpieczeństwa i dostępnego szkolenia. Typowa analiza potrzeb szkoleniowych rozpoczyna się od przeprowadzenia analizy odbiorcy, która zazwyczaj obejmuje następujące kroki:

- a) Wdrożenie SMS będzie wpływać na każdego pracownika podmiotu lotniczego, jednak nie w ten sam sposób lub w tym samym stopniu. Należy zidentyfikować grupy pracowników oraz sposoby ich interakcji z procesami zarządzania bezpieczeństwem, danymi wejściowymi i wyjściowymi – w szczególności z ich obowiązkami w zakresie bezpieczeństwa. Informacje te powinny być dostępne w opisach stanowisk/obowiązków. Zazwyczaj zaczynają się pojawiać grupy osób, które mają podobne potrzeby edukacyjne. Podmiot lotniczy powinien rozważyć, czy wskazane jest rozszerzenie analizy na pracowników zewnętrznych organizacji współpracujących;
- b) Określenie wiedzy i kompetencji potrzebnych do wykonywania każdego obowiązku w zakresie bezpieczeństwa i wymaganych przez każdą grupę personelu.
- c) Przeprowadzenie analizy w celu zidentyfikowania luki pomiędzy obecnymi umiejętnościami i wiedzą w zakresie bezpieczeństwa wśród pracowników a wiedzą i umiejętnościami niezbędnymi do skutecznej realizacji przydzielonych obowiązków w zakresie bezpieczeństwa.
- d) Określenie najbardziej odpowiedniego podejścia do rozwoju umiejętności i wiedzy dla każdej grupy w celu opracowania programu szkolenia odpowiedniego dla zaangażowania każdej osoby lub grupy w zarządzanie bezpieczeństwem. Program szkolenia powinien również uwzględniać bieżącą wiedzę pracowników na temat bezpieczeństwa i potrzeby w zakresie kompetencji; potrzeby te będą zazwyczaj zaspokajane poprzez program szkoleń okresowych.

9.6.4.5 Ważne jest również określenie odpowiedniej metody zapewniania szkoleń. Główny cel sprowadza się do tego, aby po zakończeniu szkolenia, personel był kompetentny do wykonywania swoich obowiązków SMS. Kompetentni wykładowcy są zazwyczaj czynnikiem kluczowym. Ich zaangażowanie, umiejętności dydaktyczne i wiedza w zakresie zarządzania bezpieczeństwem będą miały istotny wpływ na skuteczność prowadzonych szkoleń. Program szkolenia w zakresie bezpieczeństwa powinien również określać obowiązki dotyczące opracowania treści i harmonogramu szkolenia, a także zarządzania rejestrami w zakresie szkoleń i kompetencji.

9.6.4.6 Organizacja powinna określić, kto powinien zostać przeszkolony i do jakiego stopnia, a to będzie zależało od zakresu zaangażowania danej osoby w SMS. Większość osób pracujących w organizacji ma bezpośredni lub pośredni związek z bezpieczeństwem lotniczym, a zatem posiada obowiązki SMS. Dotyczy to każdego personelu bezpośrednio zaangażowanego w zapewnianie produktów i usług, oraz personelu zaangażowanego w prace komitetów ds. bezpieczeństwa organizacji. Niektórzy pracownicy administracyjni i pomocniczy będą mieli ograniczone obowiązki w zakresie SMS i będą potrzebować szkolenia SMS, ponieważ ich praca może mieć pośredni wpływ na bezpieczeństwo lotnicze.

9.6.4.7 Podmiot lotniczy powinien określić obowiązki personelu związane z SMS i wykorzystać te informacje do sprawdzenia programu szkolenia w zakresie bezpieczeństwa, aby upewnić się, że każda osoba przejdzie szkolenie dostosowane do jej stopnia zaangażowania w SMS. Program szkolenia w zakresie bezpieczeństwa powinien określać treść szkolenia w zakresie bezpieczeństwa dla personelu pomocniczego, personelu operacyjnego, kierowników i przełożonych, kierowników wyższego szczebla i dyrektora odpowiedzialnego.

9.6.4.8 Należy zapewnić dostępność specjalnych szkoleń w zakresie bezpieczeństwa dla dyrektora odpowiedzialnego i kierowników wyższego szczebla, które obejmują następujące zagadnienia:

- a) specjalne szkolenia uświadamiające dla nowych dyrektorów odpowiedzialnych i pracowników w zakresie odpowiedzialności i obowiązków związanych z SMS;
- b) znaczenie zgodności z krajowymi i organizacyjnymi wymaganiami bezpieczeństwa;
- c) zaangażowanie kierownictwa;
- d) alokacja zasobów;
- e) promowanie polityki bezpieczeństwa i SMS;
- f) promowanie pozytywnej kultury bezpieczeństwa;
- g) skuteczna komunikacja w zakresie bezpieczeństwa pomiędzy komórkami organizacyjnymi;
- h) cel bezpieczeństwa, SPT i poziomy alarmowe; oraz
- i) polityka dyscyplinarna.

9.6.4.9 Głównym celem programu szkolenia w zakresie bezpieczeństwa jest zapewnienie, że personel na wszystkich szczeblach organizacji utrzymuje swoje kompetencje do pełnienia funkcji w zakresie bezpieczeństwa, dlatego kompetencje personelu powinny być poddawane regularnemu przeglądowi.

9.6.5 Komunikacja w zakresie bezpieczeństwa

9.6.5.1 Podmiot lotniczy powinien rozpowszechniać wszystkie cele i procedury SMS organizacji wśród całego odpowiedniego personelu. Powinna istnieć strategia komunikacji, która umożliwi komunikację w zakresie bezpieczeństwa za pomocą najwłaściwszej metody w oparciu o rolę jednostki i konieczność uzyskania informacji dotyczących bezpieczeństwa. Można to zrealizować za pomocą broszur bezpieczeństwa, ogłoszeń, biuletynów, briefingów lub kursów szkoleniowych. Kierownik ds. bezpieczeństwa powinien również zapewnić, że wnioski wyciągnięte z badań i historii przypadków lub doświadczenia, zarówno wewnętrzne, jak i innych organizacji, są szeroko rozpowszechniane. Dlatego komunikacja w zakresie bezpieczeństwa ma na celu:

- a) *zapewnienie, że pracownicy są w pełni świadomi SMS*: jest to dobry sposób na promowanie polityki bezpieczeństwa i celów bezpieczeństwa organizacji.
- b) *przekazywanie informacji krytycznych dla bezpieczeństwa*: informacje krytyczne dla bezpieczeństwa to konkretne informacje dotyczące problemów związanych z bezpieczeństwem i ryzyk bezpieczeństwa, które mogą narazić organizację na ryzyko bezpieczeństwa. Mogą one wynikać z informacji bezpieczeństwa zebranych ze źródeł wewnętrznych lub zewnętrznych, takich jak zdobyte doświadczenia lub środki kontroli ryzyka bezpieczeństwa. Podmiot lotniczy określa zakres informacji uznawanych za krytyczne dla bezpieczeństwa oraz terminy ich rozpowszechniania.
- c) *podnoszenie świadomości na temat nowych środków kontroli ryzyka i działań naprawczych*: ryzyka bezpieczeństwa napotykanego przez podmiot lotniczy zmieniają się z upływem czasu, i niezależnie od tego czy jest to nowe ryzyko bezpieczeństwa, które zostało zidentyfikowane, czy są to zmiany w środkach kontroli ryzyka bezpieczeństwa, zmiany te będą musiały zostać przekazane odpowiedniemu personelowi.
- d) *zapewnianie informacji o nowych lub zmienionych procedurach bezpieczeństwa*: jeżeli procedury bezpieczeństwa są aktualizowane, ważne jest, aby odpowiednie osoby były świadome tych zmian.

- e) *promowanie pozytywnej kultury bezpieczeństwa i zachęcanie personelu do identyfikowania i zgłaszania zagrożeń*: komunikacja w zakresie bezpieczeństwa jest dwukierunkowa. Ważne jest, aby cały personel przekazywał problemy związane z bezpieczeństwem poprzez system zgłaszania zdarzeń dotyczących bezpieczeństwa.
- f) *przekazywanie informacji zwrotnych*: przekazywanie informacji zwrotnych personelowi składającemu zgłoszenia zdarzeń dotyczących bezpieczeństwa na temat działań podjętych w celu rozwiązania wszelkich zidentyfikowanych problemów.

9.6.5.2 Podmioty lotnicze powinny rozważyć, czy któreś z wymienionych powyżej informacji dotyczących bezpieczeństwa powinny być przekazane organizacjom zewnętrznym.

9.6.5.3 Podmioty lotnicze powinny ocenić skuteczność swojej komunikacji w zakresie bezpieczeństwa poprzez sprawdzenie, czy personel otrzymał i zrozumiał wszelkie informacje krytyczne dla bezpieczeństwa, które zostały rozpowszechnione. Można to zrobić w ramach działań audytu wewnętrznego lub oceny skuteczności SMS.

9.6.5.4 Działania związane z promocją bezpieczeństwa powinny być prowadzone przez cały cykl życia SMS-a, nie tylko na stronie początek.

9.7. PLANOWANIE WDROŻENIA

9.7.1 Opis systemu

9.7.1.1 Opis systemu pomaga zidentyfikować procesy organizacji, w tym wszelkie interfejsy, w celu określenia zakresu SMS. Daje on możliwość zidentyfikowania wszelkich luk związanych z komponentami i elementami SMS podmiotu lotniczego i może służyć jako punkt wyjścia do identyfikacji zagrożeń organizacyjnych i operacyjnych. Opis systemu służy do identyfikacji cech produktu, usługi lub działania, tak aby zarządzanie ryzykiem bezpieczeństwa oraz zapewnianie bezpieczeństwa mogły być skuteczne.

9.7.1.2 Większość organizacji składa się ze złożonej sieci interfejsów i interakcji z udziałem różnych komórek wewnętrznych oraz różnych organizacji zewnętrznych, które przyczyniają się do bezpiecznego działania organizacji. Wykorzystanie opisu systemu umożliwia organizacji uzyskanie wyraźniejszego obrazu wielu interakcji i interfejsów. Umożliwi to lepsze zarządzanie ryzykiem bezpieczeństwa i środkami kontroli ryzyka bezpieczeństwa, jeżeli zostały one opisane, i pomoże w zrozumieniu wpływu zmian w procesach i procedurach SMS.

9.7.1.3 Rozważając opis systemu, ważne jest, aby zrozumieć, że „system” jest zbiorem elementów pracujących razem jako części wzajemnie połączonej sieci. W przypadku SMS, są to produkty organizacji, ludzie, procesy, procedury, urządzenia, usługi i inne aspekty (w tym czynniki zewnętrzne), które są związane i mogą wpływać na działalność organizacji w zakresie bezpieczeństwa lotniczego. Często „system” jest zbiorem systemów, które mogą być również postrzegane jako system z podsystemami. Systemy te i ich wzajemne relacje tworzą źródła zagrożeń i wpływają na kontrolę ryzyka bezpieczeństwa. Ważne systemy obejmują zarówno te, które mogą bezpośrednio wpływać na bezpieczeństwo lotnicze, jak i te, które wpływają na zdolność lub możliwość organizacji do skutecznego zarządzania bezpieczeństwem.

9.7.1.4 Przegląd opisu systemu i interfejsów SMS powinien być zawarty w dokumentacji SMS. Opis systemu może zawierać wypunktowaną listę z odniesieniami do polityk i procedur. Zobrazowanie graficzne, takie jak schemat procesu lub schemat organizacyjny z adnotacjami, może być wystarczające dla niektórych organizacji. Organizacja powinna stosować metodę i format, który działa dla tej organizacji.

9.7.1.5 Ponieważ każda organizacja jest wyjątkowa, nie istnieje „uniwersalna” metoda wdrożenia SMS. Oczekuje się, że każda organizacja wdroży SMS, który działa w specyficznych dla niej warunkach. Każda organizacja powinna sama określić sposób, w jaki zamierza spełnić podstawowe wymagania. Aby to osiągnąć,

ważne jest, aby każda organizacja przygotowała opis systemu, który przedstawia struktury organizacyjne, procesy i ustalenia biznesowe, które uważa za ważne dla funkcji zarządzania bezpieczeństwem. Na podstawie opisu systemu organizacja powinna określić lub opracować politykę, procesy i procedury, które ustanawiają jej własne wymagania w zakresie zarządzania bezpieczeństwem.

9.7.1.6 Jeżeli organizacja zdecyduje się dokonanie znaczącej lub merytorycznej zmiany w procesach określonych w opisie systemu, zmiany te należy postrzegać jako potencjalnie wpływające na jej bazową ocenę ryzyka bezpieczeństwa. Dlatego opis systemu powinien zostać poddany przeglądowi w ramach procesów zarządzania zmianą.

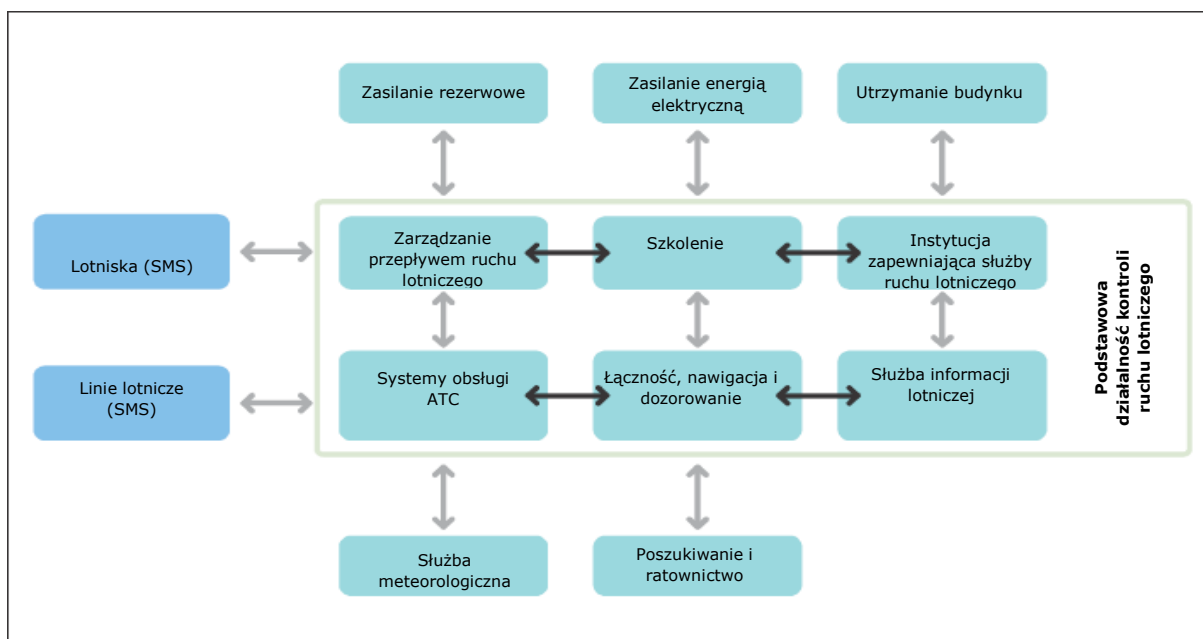
9.7.2 Zarządzanie interfejsem

Interfejsy mają wpływ na ryzyka bezpieczeństwa, na które narażone są podmioty lotnicze. Interfejsy mogą być wewnętrzne (np. pomiędzy komórkami organizacyjnymi) lub zewnętrzne (np. inne podmioty lotnicze lub podwykonawcy). Identyfikując i zarządzając tymi interfejsami, podmiot lotniczy ma większą kontrolę nad wszelkimi ryzykami bezpieczeństwa związanymi z interfejsami. Interfejsy te powinny być zdefiniowane w opisie systemu.

9.7.3 Identyfikacja interfejsów SMS

9.7.3.1 Początkowo podmioty lotnicze powinny koncentrować się na interfejsach w odniesieniu do swojej działalności gospodarczej. Interfejsy te powinny być szczegółowo przedstawione w opisie systemu, który określa zakres SMS i powinien obejmować interfejsy wewnętrzne i zewnętrzne.

9.7.3.2 Rysunek 9-3 przedstawia przykładowy sposób, w jaki podmiot lotniczy może zmapować różne organizacje, z którymi współpracuje, w celu zidentyfikowania interfejsów SMS. Ma to na celu stworzenie wyczerpującej listy wszystkich interfejsów. Uzasadnieniem dla realizacji tego ćwiczenia jest to, że mogą istnieć interfejsy SMS, których organizacja niekoniecznie jest w pełni świadoma. Mogą istnieć interfejsy, w obrębie których nie zawarto formalnych porozumień, jak ma to miejsce z firmami energetycznymi lub firmami zajmującymi się utrzymaniem budynków.



Rysunek 9-3. Przykłady interfejsów systemu zarządzania bezpieczeństwem instytucji zapewniającej służbę ruchu lotniczego

9.7.3.3 Niektóre interfejsy wewnętrzne mogą dotyczyć obszarów biznesowych niezwiązanych bezpośrednio z bezpieczeństwem, takich jak marketing, finanse, zasoby prawne i ludzkie. Obszary te mogą wpływać na bezpieczeństwo poprzez podejmowanie decyzji mających wpływ na zasoby wewnętrzne i inwestycje, a także poprzez porozumienia i umowy z organizacjami zewnętrznymi, i niekoniecznie dotyczą bezpieczeństwa.

9.7.3.4 Po zidentyfikowaniu interfejsów SMS, podmiot lotniczy powinien rozważyć ich krytyczność. Dzięki temu podmiot może nadać priorytet zarządzaniu bardziej krytycznymi interfejsami i potencjalnymi ryzykami bezpieczeństwa. Należy wziąć pod uwagę:

- a) co jest zapewniane;
- b) dlaczego jest to potrzebne;
- c) czy zaangażowane organizacje mają SMS lub inny system zarządzania; oraz
- d) czy interfejs obejmuje udostępnianie danych/informacji dotyczących bezpieczeństwa.

Ocena wpływu interfejsów na bezpieczeństwo

9.7.3.5 Podmiot lotniczy powinien następnie zidentyfikować wszelkie zagrożenia związane z interfejsami i przeprowadzić ocenę ryzyka bezpieczeństwa z wykorzystaniem istniejących procesów identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa.

9.7.3.6 Na podstawie zidentyfikowanych ryzyk bezpieczeństwa, podmiot może rozważyć współpracę z inną organizacją w celu określenia i zdefiniowania odpowiedniej strategii kontroli ryzyka bezpieczeństwa. Zaangażowanie innej organizacji przyczyni się do identyfikacji zagrożeń, oceny ryzyka bezpieczeństwa, a także określenia odpowiedniej kontroli ryzyka bezpieczeństwa. Ten wspólny wysiłek jest potrzebny, ponieważ postrzeganie ryzyk bezpieczeństwa może nie być takie samo w przypadku każdej organizacji. Kontrola ryzyka może być przeprowadzona przez podmiot lotniczy lub organizację zewnętrzną.

9.7.3.7 Należy również uwzględnić, że każda zaangażowana organizacja ma obowiązek identyfikowania i zarządzania zagrożeniami, które wpływają na ich własną organizację. Może to oznaczać, że krytyczny charakter interfejsu jest inny dla każdej organizacji, ponieważ mogą one stosować różne klasyfikacje ryzyka bezpieczeństwa i mieć różne priorytety ryzyka bezpieczeństwa (pod względem poziomu bezpieczeństwa, zasobów, czasu, itp.).

Zarządzanie interfejsami i ich monitorowanie

9.7.3.8 Podmiot lotniczy jest odpowiedzialny za zarządzanie interfejsami i ich monitorowanie w celu zapewnienia bezpieczeństwa świadczonych usług i produktów. Działania te zapewnią skuteczne zarządzanie interfejsami oraz zachowanie ich aktualności i adekwatności. Zawarcie formalnych umów stanowi skuteczny sposób osiągnięcia tego celu, ponieważ interfejsy i związane z nimi obowiązki mogą być jasno określone. Wszelkie informacje o zmianach interfejsów i związanych z nimi oddziaływań powinny być przekazywane odpowiednim organizacjom.

9.7.3.9 Wyzwania związane ze zdolnością podmiotu lotniczego do zarządzania ryzykiem bezpieczeństwa związanym z interfejsami dotyczą następujących kwestii:

- a) środki kontroli ryzyka bezpieczeństwa jednej organizacji nie są kompatybilne ze środkami kontroli ryzyka innych organizacji;
- b) gotowość obu organizacji do zaakceptowania zmian we własnych procesach i procedurach;
- c) niewystarczające zasoby lub niedostateczna wiedza techniczna do zarządzania i monitorowania interfejsu; oraz

- d) liczba i lokalizacja interfejsów.

9.7.3.10 Ważne jest, aby uznać potrzebę koordynacji pomiędzy organizacjami zaangażowanymi w interfejs. Skuteczna koordynacja powinna obejmować:

- a) wyjaśnienie ról i obowiązków każdej organizacji;
- b) uzgodnienie decyzji w sprawie działań, które należy podjąć (np. działania w zakresie kontroli ryzyka bezpieczeństwa i ramy czasowe);
- c) określenie, które informacje bezpieczeństwa muszą być udostępniane i przekazywane;
- d) ustalenie w jaki sposób i kiedy koordynacja powinna mieć miejsce (grupa zadaniowa, regularne spotkania, spotkania ad hoc lub dedykowane spotkania); oraz
- e) uzgadnianie rozwiązań, które przynoszą korzyści obu organizacjom, ale które nie wpływają negatywnie na skuteczność SMS.

9.7.3.11 Wszystkie problemy związane z bezpieczeństwem lub ryzyka bezpieczeństwa związane z interfejsami powinny być udokumentowane i udostępnione każdej organizacji w celu wymiany i przeglądu. Umożliwi to dzielenie się zdobytymi doświadczeniami i gromadzenie danych dotyczących bezpieczeństwa, które będą cenne dla obu organizacji. Korzyści w zakresie bezpieczeństwa operacyjnego można osiągnąć poprzez zwiększenie bezpieczeństwa w każdej organizacji w wyniku współwłasności ryzyk i obowiązków w zakresie bezpieczeństwa.

9.7.4 Skalowalność SMS

9.7.4.1 SMS organizacji, w tym polityki, procesy i procedury, powinien odzwierciedlać rozmiar i złożoność organizacji i jej działalności. Powinien on uwzględniać:

- a) strukturę organizacyjną i dostępność zasobów;
- b) rozmiar i złożoność organizacji (w tym wiele lokalizacji i baz); oraz
- c) złożoność działań i interfejsów z organizacjami zewnętrznymi.

9.7.4.2 Podmiot lotniczy powinien przeprowadzić analizę swoich działań w celu określenia odpowiedniego poziomu zasobów do zarządzania systemem SMS. Będzie się to wiązać z określeniem struktury organizacyjnej niezbędnej do zarządzania SMS. Dotyczy to również uwzględnienia kto będzie odpowiedzialny za zarządzanie i utrzymanie SMS, jakie komitety ds. bezpieczeństwa są potrzebne, jeżeli w ogóle, oraz uwzględnienia potrzeby konkretnych specjalistów ds. bezpieczeństwa.

Uwarunkowania związane z ryzykiem bezpieczeństwa

9.7.4.3 Niezależnie od wielkości podmiotu lotniczego, skalowalność powinna być również funkcją nieodłącznego ryzyka bezpieczeństwa w działalności podmiotu. Nawet małe organizacje mogą być zaangażowane w działania, które mogą wiązać się ze znacznym ryzykiem dla bezpieczeństwa lotniczego. Dlatego zdolność zarządzania bezpieczeństwem powinna być współmierna do ryzyka bezpieczeństwa, którym trzeba będzie zarządzać.

Dane bezpieczeństwa i informacje bezpieczeństwa oraz ich analiza

9.7.4.4 W przypadku małych organizacji, niewielka ilość danych może oznaczać, że trudniej jest zidentyfikować trendy lub zmiany w zakresie bezpieczeństwa. Może to wymagać organizowania spotkań w celu omówienia problemów związanych z bezpieczeństwem z odpowiednimi ekspertami. Działania takie mogą mieć charakter bardziej jakościowy niż ilościowy, ale pomogą zidentyfikować zagrożenia i ryzyka dla podmiotu

lotniczego. Pomocna może być współpraca z innymi podmiotami lotniczymi lub stowarzyszeniami branżowymi, ponieważ mogą one posiadać dane, których dany podmiot nie posiada. Na przykład, mniejsze podmioty lotnicze mogą wymieniać się z podobnymi organizacjami/operacjami w celu udostępniania informacji o ryzyku bezpieczeństwa i identyfikowania trendów w zakresie bezpieczeństwa. Podmioty lotnicze powinny odpowiednio analizować i przetwarzać swoje dane wewnętrzne, nawet jeżeli mają one ograniczony zakres.

9.7.4.5 Podmioty lotnicze z wieloma interakcjami i interfejsami będą musiały rozważyć sposób zbierania danych bezpieczeństwa i informacji bezpieczeństwa z wielu organizacji. Może to spowodować gromadzenie dużych ilości danych, które będą musiały być następnie powiązane i przeanalizowane. Podmioty lotnicze powinny korzystać z odpowiedniej metody zarządzania takimi danymi. Należy również wziąć pod uwagę jakość gromadzonych danych i zastosowanie taksonomii, aby pomóc w analizie danych.

9.7.5 Integracja systemów zarządzania

9.7.5.1 Zarządzanie bezpieczeństwem należy traktować jako część systemu zarządzania (a nie jako odrębny system). Dlatego podmiot lotniczy może wdrożyć zintegrowany system zarządzania, który obejmuje swoim zakresem SMS. Zintegrowany system zarządzania może być wykorzystywany do uzyskania wielu certyfikatów, upoważnień lub zatwierdzeń lub do objęcia swojej działalności innymi systemami zarządzania, takimi jak system zarządzania jakością, ochroną, bezpieczeństwem i higieną pracy oraz środowiskiem. Ma to na celu wyeliminowanie powielania wysiłków i wykorzystanie synergii poprzez zarządzanie ryzykami bezpieczeństwa w wielu działaniach. Na przykład, jeżeli podmiot lotniczy posiada wiele certyfikatów, może zdecydować się na wdrożenie jednego systemu zarządzania, który obejmie całość jego działalności. Podmiot powinien zdecydować o najlepszych środkach służących integracji lub oddzieleniu SMS w celu zaspokojenia swoich potrzeb biznesowych lub organizacyjnych.

9.7.5.2 Typowy zintegrowany system zarządzania może obejmować:

- a) system zarządzania jakością (QMS);
- b) system zarządzania bezpieczeństwem (SMS);
- c) system zarządzania ochroną (SeMS), dalsze wytyczne znajdują się w *Podręczniku ochrony lotnictwa* (Doc 8973 – dokument zastrzeżony);
- d) system zarządzania środowiskowego (EMS);
- e) system zarządzania bezpieczeństwem i higieną pracy (OHSMS);
- f) system zarządzania finansami (FMS);
- g) system zarządzania dokumentacją (DMS); oraz
- h) system zarządzania ryzykiem związanym ze zmęczeniem (FRMS).

9.7.5.3 Podmiot lotniczy może zdecydować się na zintegrowanie tych systemów zarządzania w oparciu o swoje potrzeby. Procesy zarządzania ryzykiem i procesy audytu wewnętrznego są podstawowymi cechami większości tych systemów zarządzania. Należy uznać, że ryzyka i środki kontroli ryzyka opracowane w którymkolwiek z tych systemów mogą mieć wpływ na inne systemy. Ponadto mogą istnieć inne systemy operacyjne związane z działalnością biznesową, które mogą być również zintegrowane, takie jak zarządzanie dostawcami, zarządzanie infrastrukturą, itp.

9.7.5.4 Podmiot lotniczy może również rozważyć zastosowanie SMS w innych obszarach, w których nie ma obowiązującego wymogu prawnego dotyczącego wdrożenia SMS. Podmioty lotnicze powinny określić najodpowiedniejsze środki do integracji lub oddzielenia swojego systemu zarządzania w celu dostosowania do

modelu biznesowego, środowiska operacyjnego, wymogów prawnych i ustawowych jak również do oczekiwań społeczności lotniczej. Niezależnie od wybranej opcji, należy zapewnić spełnienie wymagań w zakresie SMS.

Korzyści i wyzwania związane z integracją systemu zarządzania

9.7.5.5 Integracja różnych obszarów w ramach jednego systemu zarządzania poprawi wydajność poprzez:

- a) ograniczenie powielania i nakładania się procesów i zasobów;
- b) zmniejszenie potencjalnie sprzecznych obowiązków i relacji;
- c) uwzględnienie szerszego wpływu ryzyk i możliwości na wszystkie działania; oraz
- d) umożliwienie skutecznego monitorowania i zarządzania działaniami we wszystkich obszarach.

9.7.5.6 Możliwe wyzwania związane z integracją systemu zarządzania obejmują:

- a) istniejące systemy mogą mieć różnych kierowników funkcjonalnych, którzy sprzeciwiają się integracji, co może powodować konflikt;
- b) może istnieć opór przed zmianą wśród personelu, na który integracja wpływa, ponieważ będzie to wymagało ściślejszej współpracy i koordynacji;
- c) wpływ na ogólną kulturę bezpieczeństwa w organizacji, ponieważ mogą istnieć różne kultury w odniesieniu do każdego systemu, co może powodować konflikty;
- d) przepisy mogą uniemożliwić taką integrację lub różne organy regulacyjne i normalizacyjne mogą mieć rozbieżne oczekiwania co do sposobu spełnienia ich wymagań; oraz
- e) integracja różnych systemów zarządzania (takich jak QMS i SMS) może powodować dodatkową pracę aby wykazać, że oddzielne wymagania są spełnione.

9.7.5.7 W celu zwiększenia do maksimum korzyści płynących z integracji oraz sprostania powyższym wyzwaniom, niezbędne jest zaangażowanie i przywództwo kierownictwa wyższego szczebla dla skutecznego zarządzania zmianą. Ważne jest, aby wyznaczyć osobę, która będzie ponosić ogólną odpowiedzialność za zintegrowany system zarządzania.

9.7.6 Integracja systemu zarządzania bezpieczeństwem (SMS) i systemu zarządzania jakością (QMS)

9.7.6.1 Niektóre podmioty lotnicze posiadają zarówno SMS, jak i QMS. Są one czasami zintegrowane w jeden system zarządzania. System zarządzania jakością jest ogólnie definiowany jako struktura organizacyjna i związane z nią zakresy odpowiedzialności, zasoby, procesy i procedury niezbędne do ustanowienia i promowania systemu ciągłego zapewniania jakości oraz poprawy w zapewnianiu produktu lub usługi.

9.7.6.2 Obydwa systemy są komplementarne: SMS koncentruje się na zarządzaniu ryzykami bezpieczeństwa i poziomem bezpieczeństwa, podczas gdy QMS koncentruje się na zapewnieniu zgodności z przepisami i wymaganiami nakazowymi w celu spełnienia oczekiwań klientów i zobowiązań umownych. SMS ma na celu identyfikację zagrożeń, oceną związanego z nimi ryzyka bezpieczeństwa i wdrożenie skutecznych środków kontroli ryzyka bezpieczeństwa. Natomiast QMS koncentruje się na spójnym zapewnianiu produktów i usług, które spełniają odpowiednie specyfikacje. Niemniej jednak, zarówno SMS, jak i QMS:

- a) powinny być planowane i zarządzane;
- b) obejmują wszystkie funkcje organizacyjne związane z zapewnianiem produktów i usług lotniczych;

- c) identyfikują nieskuteczne procesy i procedury;
- d) dążą do ciągłego doskonalenia; oraz
- e) mają ten sam cel, polegający na zapewnieniu klientom bezpiecznych i niezawodnych produktów i usług.

9.7.6.3 SMS koncentruje się na:

- a) identyfikacji zagrożeń związanych z bezpieczeństwem w organizacji;
- b) ocenie związanego z nimi ryzyka bezpieczeństwa;
- c) wdrożeniu skutecznych środków kontroli ryzyka bezpieczeństwa w celu ograniczenia ryzyk bezpieczeństwa;
- d) pomiarze poziomu bezpieczeństwa; oraz
- e) utrzymaniu odpowiedniego przydziału zasobów w celu spełnienia wymagań dotyczących poziomu bezpieczeństwa.

9.7.6.4 QMS koncentruje się na:

- a) zgodności z przepisami i wymaganiami;
- b) spójności w zapewnianiu produktów i usług;
- c) spełnianiu określonych standardów działania; oraz
- d) zapewnianiu produktów i usług, które są „odpowiednie” i wolne od wad lub błędów.

9.7.6.5 Monitorowanie zgodności z przepisami jest konieczne w celu zapewnienia, że środki kontroli ryzyka bezpieczeństwa stosowane w formie przepisów, są skutecznie wdrażane i monitorowane przez podmiot prowadzący działalność w lotnictwie cywilnym. Przyczyny i czynniki sprawcze wszelkich niezgodności powinny również zostać przeanalizowane i wyeliminowane.

9.7.6.6 Biorąc pod uwagę komplementarne aspekty SMS i QMS, możliwe jest zintegrowanie obu systemów bez narażania każdej funkcji. Można to podsumować w następujący sposób:

- a) SMS jest wspierany przez procesy QMS, takie jak audyt, inspekcja, badanie, analiza przyczyn źródłowych, projektowanie procesów i działania zapobiegawcze;
- b) QMS może identyfikować problemy związane z bezpieczeństwem lub słabości w środkach kontroli ryzyka bezpieczeństwa;
- c) QMS może przewidywać problemy związane z bezpieczeństwem, które istnieją pomimo zapewnienia zgodności organizacji ze standardami i specyfikacjami;
- d) zasady jakości, polityki i praktyki powinny być dostosowane do celów zarządzania bezpieczeństwem; oraz
- e) działania QMS powinny uwzględniać zidentyfikowane zagrożenia i środki kontroli ryzyka bezpieczeństwa w planowaniu i prowadzeniu audytów wewnętrznych.

9.7.6.7 Podsumowując, w zintegrowanym systemie zarządzania z ujednoczonymi celami i procesem podejmowania decyzji, który uwzględnia szerszy wpływ na wszystkie działania, procesy zarządzania jakością i

zarządzania bezpieczeństwem będą w dużym stopniu komplementarne i będą wspierać osiągnięcie ogólnych celów bezpieczeństwa.

9.7.7 Analiza luk i wdrożenie SMS

9.7.7.1 Przed wdrożeniem SMS podmiot lotniczy powinien przeprowadzić analizę luk. Polega ona na porównaniu istniejących procesów i procedur zarządzania bezpieczeństwem podmiotu z wymaganiami w zakresie SMS określonymi przez Państwo. Jest prawdopodobne, że podmiot lotniczy posiada już pewne funkcje SMS. Rozwój SMS powinien opierać się na istniejących politykach i procesach organizacyjnych. Analiza luk identyfikuje luki, które należy wyeliminować za pomocą planu wdrożenia SMS, który określa działania niezbędne do wdrożenia w pełni funkcjonalnego i skutecznego SMS.

9.7.7.2 Plan wdrożenia SMS powinien zapewniać jasny obraz zasobów, zadań i procesów wymaganych do wdrożenia SMS. Czas i kolejność realizacji planu wdrożenia mogą zależeć od wielu czynników specyficznych dla każdej organizacji, takich jak:

- a) wymagania prawne;
- b) posiadanie wielu certyfikatów (z możliwymi różnymi datami wdrożenia przepisów);
- c) zakres, w jakim SMS może opierać się na istniejących strukturach i procesach;
- d) dostępność zasobów i budżetu;
- e) współzależności pomiędzy różnymi etapami (przed ustanowieniem systemu analizy danych, należy najpierw wdrożyć system zgłaszania zdarzeń dotyczących bezpieczeństwa); oraz
- f) istniejąca kultura bezpieczeństwa.

9.7.7.3 Plan wdrożenia SMS powinien zostać opracowany w porozumieniu z dyrektorem odpowiedzialnym i innymi kierownikami wyższego szczebla i powinien określać osoby odpowiedzialne za poszczególne działania wraz z ramami czasowymi. Plan powinien uwzględniać koordynację z organizacjami zewnętrznymi lub wykonawcami, w stosownych przypadkach.

9.7.7.4 Plan wdrożenia SMS może być udokumentowany w różnych formach, od prostego arkusza kalkulacyjnego do specjalistycznego oprogramowania do zarządzania projektami. Plan powinien być regularnie monitorowany i w razie potrzeby aktualizowany. Powinien również wyjaśniać, kiedy konkretny element można uznać za skutecznie wdrożony.

9.7.7.5 Zarówno Państwo, jak i podmiot lotniczy powinni uznać, że osiągnięcie skutecznego SMS może potrwać kilka lat. Podmioty lotnicze powinny odnosić się do swojego Państwa, ponieważ mogą istnieć wymagania dotyczące stopniowego podejścia do wdrażania SMS.

