Terroryzm – studia, analizy, prewencja, 2026, nr 9: 149–161

https://doi.org/10.4467/27204383TER.26.005.23788

Varia

# Bezpieczeństwo lotnictwa cywilnego w praktyce – systemy ochrony, kontrola i odporność operacyjna

Bohdan Paszukow

Securitas Services

Bezpieczeństwo lotnictwa cywilnego stanowi jeden z filarów funkcjonowania globalnego transportu. Wpływ na jego poprawę mają spójne procedury, nowoczesne narzędzia oraz odpowiednio zaprojektowane systemy ochrony. W ramach programów AVSEC (od ang. *aviation security*) są rozwijane standardy i praktyki mające na celu zapobieganie aktom bezprawnej ingerencji, wzmacnianie odporności infrastruktury oraz zapewnienie wysokiego poziomu kontroli ryzyka. Poszczególne państwa i organizacje międzynarodowe przyjmują różne modele organizacji systemów bezpieczeństwa – od centralnie zarządzanych po bardziej zdecentralizowane i oparte na odpowiedzialności operatorów. Ta różnorodność podejść jest szczególnie widoczna, gdy porówna się rozwiązania stosowane w Unii Europejskiej i Stanach Zjednoczonych.

## Ocena jakości bezpieczeństwa lotnictwa cywilnego w Stanach Zjednoczonych i Unii Europejskiej

Podczas przeprowadzania oceny jakości bezpieczeństwa lotnictwa cywilnego, szczególnie w przypadku międzynarodowej korporacji zajmującej się ochroną osób i mienia w różnych obszarach, niezbędne jest zrozumienie, w jaki sposób poszczególne regiony organizują swoje systemy bezpieczeństwa lotniczego. Stany Zjednoczone i Unia Europejska dążą do tych samych celów, jakimi są zapobieganie incydentom o charakterze terrorystycznym i zapewnienie bezpieczeństwa pasażerów, personelu i infrastruktury. Jednak ich realizacja różni się sposobem zarządzania systemem bezpieczeństwa, stylem tworzenia i egzekwowania regulacji, a także mechanizmami nadzoru nad operatorami. Unia Europejska opiera się na szczegółowych, jednolitych normach technicznych i procedurach. Stany Zjednoczone preferują model bardziej scentralizowany, z silną rolą Administracji Ochrony Transportu (Transportation Security Administration, TSA) i większym naciskiem kładzionym na rozwiązania oparte na wynikach i skuteczności, a nie sztywnych wymaganiach proceduralnych. Unia Europejska stosuje zatem podejście normatywne, a USA – efektywnościowe, co wiąże się z odmiennymi sposobami organizacji i kontroli systemów AVSEC.

TSA, która przejęła bezpośrednią odpowiedzialność za bezpieczeństwo lotnicze w Stanach Zjednoczonych, została utworzona w ramach Departamentu Bezpieczeństwa Krajowego (Department of Homeland Security) po wydarzeniach z 11 września 2001 r. Ustanawia ona jednolite wymagania dotyczące kontroli bezpieczeństwa, wydaje dyrektywy federalne związane z bezpieczeństwem oraz zarządza działaniami punktów kontroli w większości portów lotniczych. Taka centralizacja pozwala na szybkie dostosowanie się do pojawiających się zagrożeń przez zmiany dyrektyw. Nadzór jest sprawowany w ramach federalnych inspekcji, ukrytego testowania oraz aktualizacji procedur, np. po incydentach. System amerykański jest zatem nakazowy i zawiera szczegółowe wymagania dotyczące kontroli pasażerów i bagażu, weryfikacji personelu oraz kontroli dostępu. Kładzie nacisk na ujednolicenie i szybkość reakcji, a za zgodność z przepisami odpowiadają bezpośrednio agencje federalne.

Model UE opiera się na harmonizacji systemów bezpieczeństwa wielu suwerennych państw, które muszą wdrażać wspólne standardy AVSEC przy zachowaniu własnych struktur administracyjnych i odpowiedzialności krajowej.

Podstawowym unijnym aktem w zakresie bezpieczeństwa lotniczego jest rozporządzenie 300/2008[1], ustanawiające wspólne zasady kontroli bezpieczeństwa, kontroli dostępu i bezpieczeństwa ładunków. Uzupełnieniem tych zasad są akty wykonawcze określające standardy wydajności. Egzekwowanie przepisów leży w gestii organów krajowych w każdym państwie członkowskim, ale to Komisja Europejska nadzoruje ten proces. Przeprowadza ona kontrole, wymaga corocznych sprawozdań dotyczących zgodności i potwierdza stosowanie przez państwa członkowskie wspólnych przepisów. Tym, co wyróżnia system UE, jest ocena w ramach Common Evaluation Process (CEP), czyli opracowanego przez European Civil Aviation Conference (ECAC) programu testów, który zapewnia znormalizowane badania laboratoryjne urządzeń zabezpieczających pod kątem kryteriów wydajności. Gwarantuje to porównywalność zatwierdzeń urządzeń w poszczególnych państwach członkowskich i pozwala uniknąć fragmentarycznych ocen krajowych. Model UE umożliwia zatem państwom członkowskim spełnienie podstawowych wymagań przy jednoczesnym zachowaniu spójności transgranicznej dzięki zunifikowanym normom i nadzorowi Komisji Europejskiej.

Dużą zaletą unijnego systemu regulacji bezpieczeństwa lotniczego jest standaryzacja środków ochrony. Prawodawstwo UE pozwala koncentrować zasoby i wysiłki na obszarach najbardziej narażonych na ryzyko, a jednocześnie tworzy ramy do współpracy między państwami członkowskimi, organami regulacyjnymi, branżą lotniczą i innymi podmiotami zaangażowanymi w AVSEC. Ważną rolę w tym procesie odgrywają wspólne platformy i mechanizmy koordynacji, takie jak SAGAS (Security Advisory Group for Aviation Security), działający przy Komisji Europejskiej, czy branżowe organizacje reprezentujące sektor prywatny, np. ASSA-i (Aviation Security Services Association – International).

Ponadto system regulacyjny UE wspiera mechanizmy kontroli jakości i monitorowania zgodności w celu zapewnienia spójnego nadzoru operacyjnego i regulacyjnego.

Choć podejścia unijne i amerykańskie różnią się strukturą zarządzania, stylem regulacji i mechanizmami nadzoru, to w praktyce zbliżają się do siebie w ramach współpracy transatlantyckiej. W celu uniknięcia powielania certyfikacji i ujednolicenia procedur technicznych Federalna

[1] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) NR 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002* (Dz. Urz. UE L 97/72 z 9 IV 2008 r.).

Administracja Lotnictwa Stanów Zjednoczonych (U.S. Federal Aviation Administration) oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (European Union Aviation Safety Agency, EASA) mają podpisane umowy dwustronne. Współpraca ta obejmuje również kwestie bezpieczeństwa – wzajemne uznawanie niektórych kontroli i certyfikatów ułatwia działanie globalnych operatorów zgodnie z literą prawa.

## Ocena środków bezpieczeństwa fizycznego w lotnictwie cywilnym UE

Oceny zgodności stanowią podstawę bezpieczeństwa lotniczego. Zapewniają ustrukturyzowany sposób weryfikacji tego, czy lotniska, linie lotnicze i powiązani dostawcy usług przestrzegają przepisów międzynarodowych i krajowych, a także wytycznych innych krajowych organów lotnictwa cywilnego.

Metody oceniania, ich zakres i kryteria zmieniają się wraz z pojawianiem się nowych zagrożeń, rozwojem technologii oraz doświadczeniami wynikającymi z incydentów i audytów. Ewolucja ta dotyczy zarówno sposobów identyfikowania ryzyka, jak i narzędzi wykorzystywanych do jego analizy. Proces ten odbywa się również w ramach międzynarodowej sieci współpracy AVSEC, obejmującej instytucje takie jak International Civil Aviation Organization (ICAO), Komisja Europejska, TSA, EASA oraz organizacje i stowarzyszenia branżowe. To właśnie ta sieć umożliwia wymianę informacji, aktualizację standardów i dostosowywanie metod oceny ryzyka do globalnie zmieniającego się środowiska zagrożeń.

Jednym z najważniejszych elementów oceny zgodności jest monitoring systemów kontroli dostępu. Lotniska to złożone środowiska z dużą liczbą stref o ograniczonym dostępie. W ramach kontroli jakości ochrony lotnictwa cywilnego weryfikuje się, czy dostęp do obszarów wrażliwych ma tylko upoważniony personel, czy systemy identyfikacji, kontrole biometryczne i technologie nadzoru działają prawidłowo oraz czy procedury wydawania i zarządzania uprawnieniami dostępu są skuteczne. Wyklucza to sytuacje, w których dostęp uzyskałyby nieupoważnione osoby, co mogłoby narazić na niebezpieczeństwo samolot, pasażerów albo ładunek.

Równie ważna jest ocena procedur kontroli pasażerów i bagażu. W ramach oceny zgodności sprawdza się, czy technologie wykorzystywane do kontroli, takie jak urządzenia rentgenowskie, systemy wykrywania materiałów wybuchowych i skanery ciała, są odpowiednio skalibrowane

i konserwowane. Kontrola jakości obejmuje również obserwację, czy personel podczas pracy konsekwentnie przestrzega protokołów oraz zachowuje czujność.

Kolejny istotny obszar oceny to bezpieczeństwo ładunków i łańcucha dostaw, który obejmuje kontrolę sposobu sprawdzania, przechowywania i transportu ładunków. W ramach oceny weryfikuje się, czy dostawcy i kontrahenci przestrzegają zatwierdzonych praktyk bezpieczeństwa oraz czy istnieje przejrzysty łańcuch nadzoru nad wszystkimi towarami wprowadzanymi do samolotu.

Siła systemu bezpieczeństwa zależy od ludzi, którzy go wdrażają, dlatego procesy kontroli jakości kładą nacisk na ciągłą edukację, ćwiczenia i oceny personelu. Musi być on przygotowany do właściwego reagowania na podejrzane zachowania, sytuacje awaryjne lub próby naruszenia bezpieczeństwa. Oceny zgodności często obejmują symulowane scenariusze, na podstawie których sprawdza się gotowość i odporność na zagrożenia.

Ważną rolę odgrywają systemy zarządzania ryzykiem i zgłaszania incydentów. Oceny zgodności zapewniają efektywne funkcjonowanie mechanizmów identyfikacji słabych punktów, szybkiego zgłaszania naruszeń i wdrażania działań naprawczych. Dzięki kontroli jakości można śledzić szybkość i skuteczność reakcji organizacji na zidentyfikowane ryzyka, czyli wprowadzenie zmian w procedurach, technologii czy szkoleniach. Tworzy to tzw. pętlę informacji zwrotnej. Zdobyte w ten sposób doświadczenia wzmacniają bezpieczeństwo fizyczne w lotnictwie.

Kolejny ważny element to integracja technologii. W ramach oceny zgodności sprawdza się, czy systemy nadzoru, identyfikacja biometryczna i automatyczne kontrole dostępu są zainstalowane oraz aktywnie monitorowane i konserwowane. Kontrola jakości zapewnia, że dane z tych systemów wykorzystuje się do skutecznego wykrywania anomalii i zapobiegania naruszeniom.

Jednym z najbardziej bezpośrednich i praktycznych narzędzi w procesie oceny zgodności są obserwacje przeprowadzane przez audytorów i inspektorów wdrażania procedur bezpieczeństwa w czasie rzeczywistym. Dotyczy to np. zarządzania punktami kontroli dostępu czy konsekwentnego stosowania kontroli identyfikacji lub sposobu przeprowadzania kontroli bagażu. Obserwacje mogą ujawnić ewentualne rozbieżności między procedurami a praktyką.

Obserwację uzupełnia weryfikacja dokumentów, w ramach której jest sprawdzana zgodność polityk, instrukcji operacyjnych i dokumentów

organizacji z wymogami regulacyjnymi. Obejmuje to przegląd dokumentacji szkoleń mający potwierdzić, że personel otrzymał wymagane instrukcje, sprawdzanie rejestrów incydentów w celu weryfikacji, czy naruszenia są zgłaszane i badane, oraz potwierdzanie zgodności sprzętu z normami. Bez dokładnej i aktualnej dokumentacji nawet najlepsze praktyki operacyjne są niezgodne z przepisami. Ponadto przegląd dokumentów dostarcza dowodów na to, że organizacja nie tylko przestrzega przepisów obowiązujących w danym momencie, lecz także posiada systemy umożliwiające aktualizację przepisów w przyszłości.

Wywiad z personelem pomaga ocenić jego poziom zrozumienia ryzyka, nastawienie do pracy oraz gotowość do działania. Te rozmowy, zwłaszcza z funkcjonariuszami ochrony, mogą ujawnić, czy szkolenia były skuteczne oraz czy pracownicy, stosując obowiązujące procedury, czują sie pewnie. Wywiad z kadrą zarządzającą może natomiast pokazać, na ile poważnie kierownictwo traktuje kwestie bezpieczeństwa oraz czy w organizacji istnieje kultura odpowiedzialności. Co istotne, takie spotkania odsłaniają obszary, których nie da się wychwycić jedynie na podstawie dokumentów i obserwacji – np. czy personel czuje się komfortowo podczas wykonywania swoich obowiązków, szczególnie w godzinach największego natężenia ruchu, czy procedury służące do zgłaszania podejrzanych aktywności są jasne i czy kanały komunikacji budzą zaufanie.

Testowanie procedur można podzielić na metody jawne i ukryte. Testy jawne obejmują zaplanowane ćwiczenia, takie jak próbne ewakuacje czy kontrolowane próby dostępu, podczas których personel jest świadomy, że podlega ocenie. Tego typu testy mierzą poziom zgodności w obserwowanych warunkach i pomagają organizacjom doskonalić swoje procedury. Testy ukryte, określane jako red teaming, polegają na symulowaniu zagrożeń bez wcześniejszego uprzedzenia – np. przez próbę uzyskania nieautoryzowanego dostępu lub wprowadzenia przez punkty kontroli przedmiotów zabronionych. Jest to niezwykle cenne, ponieważ pokazuje funkcjonowanie systemów w warunkach rzeczywistej presji, bez sztuczności typowej dla zainscenizowanych ćwiczeń. Przeprowadzanie testów jawnych i ukrytych pokazuje, czy środki bezpieczeństwa fizycznego są zgodne z wymaganymi normami oraz skuteczne w obliczu prawdziwych zagrożeń.

Docelowo ocena zgodności i kontrola jakości bezpieczeństwa w lotnictwie cywilnym służy stworzeniu wieloaspektowego systemu ochrony. Przestrzeganie przepisów, kontrola dostępu, kontrola bezpieczeństwa, bezpieczeństwo ładunku, szkolenie personelu, zarządzanie ryzykiem i integracja

technologii razem tworzą kompleksową ochronę przed zagrożeniami. Takie podejście pozwala na utrzymanie na akceptowalnym poziomie bezpieczeństwa fizycznego w lotnictwie cywilnym. Chroni pasażerów, personel i mienie, a jednocześnie utrzymuje zaufanie publiczne do podróży lotniczych.

## Wykorzystanie sztucznej inteligencji do zapewnienia bezpieczeństwa lotnictwa cywilnego

W celu zwiększenia efektywności, dokładności oraz zdolności adaptacji systemów bezpieczeństwa lotnictwa do zmieniających się zagrożeń i warunków operacyjnych coraz częściej jest z nimi integrowana sztuczna inteligencja (ang. *artificial intelligence*, AI).

Technologie kontroli pasażerów i bagażu wykorzystują obecnie algorytmy uczenia maszynowego do skuteczniejszego wykrywania przedmiotów zabronionych niż tradycyjne systemy rentgenowskie. Narzędzia oparte na AI mogą analizować ogromne ilości danych obrazowych, rozpoznawać wzorce i charakterystykę zagrożeń oraz z większą precyzją wykrywać anomalie, co zmniejsza ryzyko błędu. Podobnie systemy identyfikacji biometrycznej stosowane na lotniskach, takie jak rozpoznawanie twarzy czy skanowanie odcisków palców, wykorzystują AI do szybkiego i bezpiecznego dopasowywania tożsamości, usprawniając w ten sposób przepływ pasażerów przy jednoczesnym utrzymaniu ścisłej kontroli dostępu.

AI jest stosowana w systemach nadzoru i monitoringu. Nowoczesne sieci monitoringu wizyjnego CCTV (od ang. *closed circuit television*) są wzbogacane o analitykę opartą na AI, która w czasie rzeczywistym potrafi wykrywać podejrzane zachowania, bagaż pozostawiony bez nadzoru czy nieautoryzowany dostęp. Ta proaktywna zdolność pozwala personelowi bezpieczeństwa szybciej i skuteczniej reagować na potencjalne zagrożenia. W bezpieczeństwie ładunków oraz w ochronie łańcucha dostaw narzędzia AI są wykorzystywane do śledzenia przesyłek, weryfikowania ich autentyczności oraz identyfikowania nieprawidłowości w procesie ich transportu.

W praktyce AI nie zastępuje tradycyjnych środków bezpieczeństwa, lecz je wspiera. Nadzór człowieka pozostaje niezbędny, ponieważ systemy AI muszą być nieustannie testowane, weryfikowane i monitorowane, aby działały w różnych warunkach. Połączenie eksperckiej wiedzy personelu z narzędziami opartymi na AI tworzy wielowarstwowy system obronny,

który wzmacnia bezpieczeństwo lotnictwa bez naruszania przy tym obowiązujących standardów.

## Elementy programu bezpieczeństwa lotnictwa korporacyjnego

Lotnictwo ma wymiar globalny, dlatego programy AVSEC w lotnictwie korporacyjnym muszą być zgodne z międzynarodowymi standardami, przepisami regionalnymi oraz wymaganiami krajowych organów lotnictwa cywilnego. Uregulowane środowisko kształtuje każdy aspekt programu – od opracowywania polityk, przez realizację operacyjną, aż po kontrolę jakości przeprowadzaną przez zewnętrzne organy nadzorcze. Organizacje tworzą też wewnętrzne mechanizmy kontroli jakości, które obejmują weryfikację dokumentacji, obserwacje operacyjne, ustrukturyzowane wywiady z personelem oraz zarówno jawne, jak i ukryte testy procedur. Włączając te procesy do codziennej działalności, organizacje mogą wcześnie identyfikować luki, korygować nieprawidłowości oraz wykazywać przed organami regulacyjnymi, że spełniają wymagane standardy lub nawet je przewyższają. Taka proaktywna kultura zgodności jest charakterystyczną cechą bezpieczeństwa lotnictwa i rzadziej występuje w innych sektorach bezpieczeństwa prywatnego, gdzie nadzór bywa mniej rygorystyczny.

Zagrożenia dla bezpieczeństwa lotnictwa ewoluują, dlatego organizacje w ramach programu bezpieczeństwa muszą inwestować w szkolenia, budowanie świadomości oraz rozwój umiejętności pracowników na wszystkich poziomach organizacji. Personel pierwszej linii (ang. *frontline workers*) potrzebuje regularnych szkoleń dotyczących procedur kontroli, a kadra zarządzająca – w zakresie reagowania kryzysowego oraz aktualizacji przepisów. Budowanie zdolności obejmuje również adaptację technologiczną – zapewnia, że personel potrafi obsługiwać zaawansowany sprzęt do kontroli bezpieczeństwa oraz reagować na pojawiające się zagrożenia w cyberprzestrzeni. Nacisk na ciągłe kształcenie się sprawia, że organizacja pozostaje odporna na nowe wyzwania, a jednocześnie odzwierciedla on dynamiczny charakter bezpieczeństwa lotnictwa korporacyjnego w porównaniu z bardziej statycznymi środowiskami bezpieczeństwa prywatnego. Większość programów bezpieczeństwa prywatnego ogranicza się do kontekstu lokalnego lub krajowego i nie wymaga tak wysokiego poziomu koordynacji międzynarodowej.

Równie ważna jest rola globalnej wymiany informacji i współpracy sieciowej między organizacjami działającymi w sektorze lotnictwa. Korporacyjne programy AVSEC korzystają z globalnych sieci, które umożliwiają dzielenie się informacjami, najlepszymi praktykami oraz wnioskami wyciągniętymi z doświadczeń. Taka komunikacja, niezależnie od tego, czy odbywa się między stowarzyszeniami branżowymi, grupami roboczymi organów regulacyjnych czy w ramach partnerstw bilateralnych, pomaga organizacjom lepiej przewidywać zagrożenia, wdrażać sprawdzone strategie oraz dostosowywać swoje działania do światowych standardów.

## Audyty bezpieczeństwa i cyberbezpieczeństwa obiektów infrastruktury krytycznej – potencjalne błędy

Dnia 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa[2]. Jej celem było dostosowanie krajowych regulacji do unijnej dyrektywy NIS 2[3] przez zwiększenie zakresu obowiązków operatorów infrastruktury krytycznej (IK). Nowe przepisy obejmują znaczną liczbę podmiotów, w tym operatorów w sektorach takich jak energetyka, transport, ochrona zdrowia oraz usługi cyfrowe.

Jednym ze wspomnianych obowiązków jest przeprowadzanie zewnętrznych audytów bezpieczeństwa systemu informacyjnego. Skuteczność audytu w zakresie wzmocnienia odporności IK zależy od podejścia organizacji do takiej kontroli.

Przede wszystkim nie należy traktować audytów jedynie jako formalnego dostosowania do wymagań. Dyrektywa NIS 2 kładzie nacisk na ciągłe zarządzanie ryzykiem, a nie tylko okresowe kontrole. Organizacje powinny włączać wnioski z audytów do swojej strategii cyberbezpieczeństwa, tak aby wprowadzane usprawnienia były trwałe, a nie tymczasowe.

Kolejnym poważnym błędem jest ignorowanie ryzyk związanych z łańcuchem dostaw oraz podmiotami trzecimi. Dyrektywa NIS 2 wymaga od operatorów oceny ryzyk wynikających ze współpracy z dostawcami

[2] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (DzU z 2026 r. poz. 20, ze zm.).

[3] *Dyrektywa 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)* – (Dz. Urz. UE L 333/80 z 27 XII 2022 r.).

i usługodawcami. Wiele systemów IK opiera się na zewnętrznych wykonawcach odpowiedzialnych za oprogramowanie, sprzęt lub utrzymanie systemów. Jeśli audyty nie oceniają tych zależności, atakujący mogą wykorzystać słabe ogniwa znajdujące się poza bezpośrednią kontrolą organizacji.

Bardzo ważne jest dopilnowanie obowiązków związanych z raportowaniem incydentów oraz reagowaniem na nie. Dyrektywa NIS 2 wymaga terminowego zgłaszania incydentów cyberbezpieczeństwa do właściwych organów krajowych. Jeśli audyty nie testują zdolności reagowania na incydenty – takich jak ścieżki eskalacji, protokoły komunikacji czy współpraca z organami regulacyjnymi – organizacje mogą nie sprostać wymaganiom w sytuacji rzeczywistego kryzysu. Audyty powinny obejmować również symulacje, które pozwolą zweryfikować poziom gotowości. Wreszcie organizacje powinny łączyć audyt z planowaniem odporności.

Uzupełnieniem dyrektywy NIS 2 jest dyrektywa CER[4], która koncentruje się na odporności fizycznej i operacyjnej podmiotów krytycznych. Jeśli audyty obejmują wyłącznie techniczne aspekty cyberbezpieczeństwa, a pomijają szersze działania zwiększające odporność – takie jak redundancja systemów, plany odtwarzania awaryjnego (ang. *disaster recovery*) czy koordynacja międzysektorowa – to IK może być narażona na ryzyka systemowe.

Podsumowując, obowiązkowe zewnętrzne audyty bezpieczeństwa IK w Polsce, gdy podejdzie się do nich strategicznie, mogą być bardzo skutecznym narzędziem. Najważniejsze kroki to rzetelne podejście do zgodności z przepisami, uwzględnianie ryzyk w łańcuchu dostaw, zapewnienie odpowiedzialności w ramach systemu zarządzania, testowanie zdolności reagowania na incydenty oraz wprowadzenie planowania odporności.

## Budowanie odporności na zagrożenia w lotnictwie cywilnym w UE – rekomendacje

Budowanie w krajach UE odporności lotnictwa cywilnego na zagrożenia wymaga kompleksowego i wielowarstwowego podejścia, które łączy nadzór regulacyjny, innowacje technologiczne oraz przygotowanie personelu. Fundament systemu stanowi przestrzeganie międzynarodowych i europejskich przepisów dotyczących bezpieczeństwa lotnictwa. Jednak odporność

[4] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE* (Dz. Urz. UE L 333/164 z 27 XII 2022 r.).

wykracza poza samą zgodność z przepisami – konieczne są proaktywne zarządzanie ryzykiem oraz zdolność do szybkiego dostosowywania się do zmieniających się zagrożeń.

Jednym z najważniejszych elementów jest wspomniana integracja zaawansowanych technologii. Systemy nadzoru wspierane przez AI, identyfikacja biometryczna przy obsłudze pasażerów czy zautomatyzowane narzędzia do kontroli ładunków przyczyniają się do skuteczniejszego wykrywania i minimalizowania ryzyka. Nieodzowne pozostaje ciągłe szkolenie oraz ocena kompetencji personelu.

Zagrożenia bezpieczeństwa często mają charakter transgraniczny, a odporność systemu zależy od terminowej wymiany informacji między organami krajowymi, liniami lotniczymi i lotniskami. Ponadto niemal każdy aspekt funkcjonowania lotnictwa wspierają systemy cyfrowe, dlatego tak istotne jest cyberbezpieczeństwo, w tym ochrona sieci przed cyberatakami oraz zapewnienie ciągłości operacji w przypadku ich zaistnienia.

Odporność na zagrożenia buduje się przez kulturę ciągłego doskonalenia. Raportowanie incydentów, audyty oraz pętla informacji zwrotnej pozwalają szybko identyfikować i eliminować słabości. Skuteczne jest podejście, w którym regulacje, technologie, wiedza i doświadczenie personelu oraz współpraca sektorowa się uzupełniają. Zaniedbanie któregokolwiek z tych filarów osłabiłoby system, ale razem tworzą one solidną tarczę, która zapewnia, że lotnictwo w krajach UE pozostaje bezpieczne, elastyczne i cieszy się zaufaniem społeczeństwa.

Jednym z największych wyzwań w ochronie lotnisk przed terroryzmem i sabotażem jest wykrywanie insiderów. Tego typu osoby zwykle działają z powodów ideologicznych, pod przymusem lub są motywowane finansowo, a ich działania mogą być trudne do wykrycia. W tym zakresie obowiązują obecnie minimalne standardy określone w rozporządzeniu 300/2008. Obejmują one m.in. rygorystyczne sprawdzanie przeszłości pracowników, ciągłe monitorowanie personelu mającego dostęp do obszarów ograniczonego dostępu oraz obowiązkowe szkolenia z zakresu bezpieczeństwa. Lotniska są zobowiązane do wdrażania systemów kontroli dostępu, przeprowadzania wyrywkowych kontroli personelu oraz egzekwowania zgłoszeń podejrzanych zachowań. Dla budowania odporności niezbędne jest wzmacnianie tych wytycznych.

Eksperci podkreślają, że w organizacjach lotniczych powinien być kładziony większy nacisk na kulturę bezpieczeństwa, która zachęca pracowników do zachowania czujności, zgłaszania niepokojących sytuacji, a także

pozwala zrozumieć ryzyko związane z nadużywaniem uprawnień ze strony współpracowników. Organizacje powinny tworzyć środowisko, w którym pracownicy czują się odpowiedzialni za bezpieczeństwo i mają pełną świadomość zagrożeń.

## Wykorzystanie rozwiązań stosowanych w lotnictwie cywilnym UE do budowania odporności na zagrożenia hybrydowe w transporcie morskim i kolejowym

Coraz większe wyzwanie dla transportowej IK stanowią zagrożenia hybrydowe, które łączą taktyki fizyczne, w cyberprzestrzeni, informacyjne, a nawet instrumenty prawne. Porty morskie i sieci kolejowe, podobnie jak lotniska, są powiązanymi systemami, których funkcjonowanie może zostać zakłócone przez sabotaż, w tym cyberataki, kampanie dezinformacyjne lub działania insiderów. Choć każdy sektor funkcjonuje we własnych realiach operacyjnych, to dorobek bezpieczeństwa lotnictwa cywilnego UE oferuje praktyki zwiększające odporność, które można zastosować w transporcie morskim i kolejowym w celu wzmocnienia ich bezpieczeństwa.

Jedną z najcenniejszych lekcji, jakie można czerpać z rozwiązań stosowanych w lotnictwie, jest przyjęcie wieloaspektowego podejścia do bezpieczeństwa opartego na ryzyku. Ochrona lotnictwa łączy wiele elementów – od kontroli pasażerów i sprawdzania ładunków po kontrolę dostępu i monitoring. To samo podejście można zastosować w transporcie morskim i kolejowym, dostosowując środki kontroli do kluczowych węzłów, takich jak terminale portowe, centra sterowania ruchem czy magazyny i terminale towarowe. Operatorzy powinni wdrażać elastyczne działania oparte na analizie wywiadowczej, które uwzględniają otwarty charakter portów i sieci kolejowych.

Warta wprowadzenia jest także dyscyplina w zakresie kontroli dostępu i systemów identyfikacyjnych. W lotnictwie wymaga się rygorystycznych sprawdzeń przeszłości pracowników, ciągłego monitorowania stref zastrzeżonych oraz wyrywkowych kontroli personelu mającego do nich dostęp. W transporcie morskim i kolejowym podobne środki mogą chronić pomieszczenia sterowania, zaplecza utrzymaniowe oraz obiekty przeładunku towarów. Zarządzanie ryzykiem wewnętrznym nie powinno ograniczać się do jednorazowej weryfikacji pracownika, lecz obejmować także monitorowanie jego zachowań oraz przeprowadzanie oceny okresowej

w celu wykrycia zmian w jego sytuacji życiowej, które mogą budzić niepokój w kontekście bezpieczeństwa organizacji.

W lotnictwie ważna jest też kultura bezpieczeństwa. Ciągłe szkolenia, ćwiczenia oparte na scenariuszach oraz obowiązek zgłaszania podejrzanych zachowań pomagają tworzyć kadrę czujną i przygotowaną na zagrożenia. Operatorzy transportu morskiego i kolejowego mogą skorzystać na przyjęciu takiej kultury, aby mieć pewność, że pracownicy rozumieją zagrożenia hybrydowe i czują się upoważnieni do reagowania na nieprawidłowości. Wspólne ćwiczenia międzysektorowe z udziałem operatorów, organów regulacyjnych i służb ratunkowych wykorzystujące symulacje zagrożeń hybrydowych wzmacniają gotowość do reagowania.

Warto jednak podkreślić, że nie wszystkie praktyki, które skutecznie działają w lotnictwie, sprawdzą się w środowiskach transportu morskiego i kolejowego. Dotyczy to np. lotniskowych punktów kontroli. Przełożenie tych rozwiązań do otwartych środowisk transportu morskiego i kolejowego prowadziłoby do powstawania wąskich gardeł i nie rozwiązałoby problemów wynikających ze specyficznych podatności tych sektorów. Podobnie nadmierne poleganie na technologii bez odpowiedniego zarządzania i nadzoru człowieka może uczynić systemy podatnymi na manipulacje ze strony przeciwnika. Rozdzielone obowiązki należy zastąpić wspólnymi strukturami dowodzenia oraz współdziałającymi protokołami współpracy między agencjami.

Łącząc sprawdzone ramy wypracowane w lotnictwie z dostosowaniami specyficznymi dla danego sektora, UE może zbudować solidną tarczę chroniącą przed kampaniami hybrydowymi wymierzonymi w jej kluczowe systemy transportowe.

Bohdan Paszukow

Specjalista w zakresie lotnictwa cywilnego, autor publikacji naukowych dotyczących bezpieczeństwa lotnisk i kontroli w lotnictwie cywilnym.

**Kontakt:** bohdan.paszukow@gmail.com