Gabriel Nowacki, Bohdan Paszukow
Wojskowa Akademia Techniczna w Warszawie

PROBLEMY BEZPIECZEŃSTWA MIĘDZYNARODOWYCH PORTÓW LOTNICZYCH

STRESZCZENIE

Celem artykułu jest przedstawienie problemów dotyczących zmian w zakresie bezpieczeństwa międzynarodowych portów lotniczych.

Z powodu nowych rodzajów zagrożeń oraz znacznego wzrostu liczby pasażerów, wprowadzane są nowe rozwiązania technologiczne które wpływają na bezpieczeństwo stref zastrzeżonych oraz ogólnodostępnych.

Problem ten ze względu na swoją złożoność oraz nieprzewidywalność wciąż pozostawia szeroką przestrzeń do wprowadzania ulepszeń oraz podnoszenia ich skuteczności.

Na podstawie przeprowadzonych badań, postawiono hipotezę roboczą, że kompetencje zawodowe pracowników oraz odpowiedni dobór elektronicznych urządzeń wspomagających, odgrywają istotne znaczenie dla stanu bezpieczeństwa międzynarodowych portów lotniczych.

Słowa kluczowe:
bezpieczeństwo, terroryzm, lotnictwo, nowe technologie

WSTĘP

Lotniska są bardzo wymagającym otoczeniem: sezonowy ruch, zmienna liczba pasażerów i zmiany w ostatniej chwili oznaczają, że wymagana jest duża elastyczność, aby sprostać specyficznym potrzebom wszystkich klientów portów lotniczych, zarówno linii lotniczych jak i podróżnych.

Ponadto, aby zdołać stawić czoła wyzwaniom związanym ze zwiększonymi przepisami bezpieczeństwa i rosnącą liczbą pasażerów oraz aby być na bieżąco z najnowszymi zagrożeniami terrorystycznymi, porty lotnicze w Europie i na świecie, poszukują coraz to nowych rozwiązań technologicznych dostosowanych do indywidualnych potrzeb zarówno ich samych jak i ich klientów, czyli pasażerów.

Porty lotnicze oraz inne podmioty uczestniczące aktywnie w budowie bezpiecznego systemu portu lotniczego, muszą zawsze brać pod uwagę czynnik ludzki, który odgrywa nadal istotną rolę, choć w erze postępujących najnowszych technologii, już nie najważniejszą.

CHARAKTERYSTYKA WYBRANYCH PROBLEMÓW BEZPIECZEŃSTWA

Bezpieczeństwo międzynarodowego portu lotniczego polega na zapewnieniu szczelności stref zastrzeżonych oraz zabezpieczeniu stref ogólnodostępnych, zależy od kompetencji zawodowych pracowników ochraniających oraz właściwego doboru elektronicznych urządzeń wspomagających.

Kompetencje zawodowe pracowników ochraniających obejmują wiedzę, doświadczenie oraz podnoszenie kwalifikacji przez personel, w zakresie monitorowania i nadzoru operacyjnego oraz kontroli jakości w ramach realizowanych zadań.

Rozwój nowych technologii wymusza odpowiedni dobór, współmierny do analizy ryzyka, elektronicznych urządzeń wspomagających w tym sprzętu, metod i środków technicznych oraz utrzymywanie ich we właściwym stanie technicznym.

Porty lotnicze są zatem idealnym poligonem doświadczalnym do zintegrowania nowych technologii w celu czerpania korzyści z globalnego wzrostu ruchu pasażerskiego i przyciągnięcia dalszych bezpośrednich lub pośrednich inwestycji. Porty lotnicze stają się stopniowo centrami innowacji i polem doświadczalnym dla najnowszych technologii, które, jeśli sprawdzą się w warunkach bezpieczeństwa lotniczego, będą miały swoje zastosowanie w innych obszarach. Wystawy, wydarzenia sportowe i rosnący ruch osobowy stwarzają dobre możliwości modernizacji infrastruktury portów lotniczych i przyjęcia technologii, które mogą poprawić doświadczenia pasażerów, jak i również bezpieczeństwo również poza samą infrastrukturą lotniskową.

Zagrożenia dla lotnictwa cywilnego

Międzynarodowe Zrzeszenie Przewoźników Powietrznych - IATA (International Air Transport Association)[1] podało, że w 2018 roku na lotniskach międzynarodowych odprawiono 4,4 miliarda pasażerów.

[1] More Connectivity and Improved Efficiency - 2018 Airline Industry Statistics Released, https://www.iata.org/pressroom/pr/Pages/2019-07-31-01.aspx#__prclt=zTkSP6TZ, 31 July 2019.

Międzynarodowa Rada Portów Lotniczych - ACI (Airports Council lnternational)[2] podała, że globalny ruch pasażerski osiągnął w 2018 roku 8,8 miliarda, co stanowi wzrost o 6,4% w stosunku do 2017 roku.

Rozbieżności w tym zakresie związane są z faktem, że linie lotnicze jako przewoźnicy zrzeszeni w IATA stosują wskaźnik pasażerski przy wylocie z danego portu, natomiast porty lotnicze zrzeszone w ACI liczą i analizują obsługę pasażerską zarówno przy wylocie z danego portu, jak i przylocie oraz tranzycie.

W 2018 r. terroryzm nadal stanowił poważne zagrożenie dla bezpieczeństwa w państwach członkowskich UE. Przerażające ataki dokonywane przez dżihadystów, takich jak te z Trèbes, Paryża, Liège i Strasburga, spowodowały śmierć łącznie trzynastu osób i wiele innych obrażeń. Terroryści mają na celu nie tylko zabijanie i okaleczanie, ale także dzielenie naszych społeczeństw i szerzenie nienawiści. Siły odpowiedzialne za bezpieczeństwo muszą zachować czujność, jeśli mają chronić obywateli i wartości w obliczu prób wykorzystania przemocy do celów politycznych.

W odniesieniu do ekosystemów portów lotniczych, niezbędnym jest podejmowanie działań mających na celu odwrócenie uwagi od punktów kontrolnych w kierunku obszarów publicznych w portach lotniczych, aby przystosować się do zmieniającego się zagrożenia, czego przykładem jest spora liczba niedawnych ataków. Istotą nowych założeń nie powinno już być skupianie uwagi jedynie na zapobieganiu przedostania się przedmiotów niebezpiecznych do stref krytycznych portów lotniczych, lecz również skoncentrowania się na obydwu stronach punktu kontrolnego, czyli w miejscach *de facto* publicznych, gdzie przecinają się systemy transportu lotniczego i naziemnego takie jak szybka kolej, metro czy punkty obsługi pasażerskiej transportu naziemnego autobusy czy samochody.

Od chwili ataków z 11 września, kraje i porty lotnicze na całym świecie wzmocniły środki bezpieczeństwa na lotniskach. Jednakże na przestrzeni ostatnich kilku lat, ataki terrorystów coraz częściej skupiają się na obszarach, gdzie ludzie nie są poddawani kontroli bezpieczeństwa, takich jak strefy odbioru bagażu lub strefy odprawy biletowej. Podwójne ataki na lotniskach i dworcach kolejowych w Brukseli w marcu 2016 r. z wykorzystaniem tej taktyki zabiły 32 osoby i trzech napastników. Powyższe świadczy o tym, iż stoimy w obliczu ambitnych przeciwników, którzy nieustannie poszukują miejsca ataku zarówno w świecie realnym jak i cyberprzestrzeni i jedynie czekają na okazję, aby ponownie uderzyć.[3]

[2] ACI report 6.4% growth in global passenger traffic, https://www.airport-technology.com/news/global-passenger-traffic-aci-report. 17 September 2019.

[3] Shapiro D., *How did security measures fail in Brussels*, John Jay College of Criminal Justice, March 2016.

Mając na uwadze obecny katalog zagrożeń wymierzonych w porty lotnicze, istnieje ciągła potrzeba aktualizacji i wzmacniania rozwiązań w zakresie bezpieczeństwa, poprzez wykorzystanie nowej oceny dzisiejszych zagrożeń oraz szybszej modyfikacji strategii bezpieczeństwa w obszarach portów lotniczych. Poniżej autorzy przedstawiają kilka kluczowych wyzwań oraz trendów związanych z rozwojem nowych technologii na rzecz bezpieczeństwa portów lotniczych oraz w stosunku do ich ekosystemów oraz infrastruktury punktów kontrolnych.

Kontrola bezpieczeństwa bagażu kabinowego

Wyjmowanie większych urządzeń elektronicznych, laptopów, ładowarek, płynów oraz żeli z bagażu podręcznego w celu zaprezentowania ich osobno do kontroli bezpieczeństwa znajduje się na czele tych czynności, które raczej negatywnie wpływają na postrzeganie jakości podróży przez pasażerów. Procedury przygotowania do procesu kontroli bezpieczeństwa niewątpliwie zajmują czas, a ten w przypadku operacji lotniczych jak i samej ekonomii funkcjonowania portu lotniczego odgrywa znaczącą rolę. Jednakże wraz z postępem technologicznym, już dziś dostępne są rozwiązania kontroli bezpieczeństwa bagażu kabinowego, która w oparciu o technologie zaczerpnięte z rozwiązań już funkcjonujących w stosunku do bagażu rejestrowanego, bądź ładunków, są dostępne w pasażerskich punktach kontroli bezpieczeństwa. Wspomniane technologie, są wdrażane przez wiodących dostawców usług w zakresie kontroli bezpieczeństwa w oparciu m.in. o rozwiązania zaczerpnięte wprost z tomografii komputerowej. Dla przykładu w wybranych portach lotniczych w Europie jak i USA, testowane są i wdrażane rozwiązania z wykorzystaniem sztucznej inteligencji, które są w stanie odróżnić materiały wybuchowe i broń od przedmiotów innych niż niebezpieczne, co pomaga operatorom kontroli bezpieczeństwa podejmować lepsze decyzje i usprawnić proces kontroli bezpieczeństwa.

Szybszy przepływ pasażerów i kontrole bezpieczeństwa mają pozytywny wpływ na ogólne doświadczenia pasażerów w porcie lotniczym i prowadzenie operacji lotniczych, przynosząc bezpośrednie korzyści finansowe wszystkim zainteresowanym stronom.

Nie bez znaczenia dla powyższego rozwoju technologicznego, okazał się wprowadzony w 2017 roku przez rząd brytyjski zakaz transportu urządzeń elektronicznych w kabinie samolotu w przypadku lotów z niektórych krajów Bliskiego Wschodu i Afryki Północnej. W wyniku tego pasażerowie lecący z niektórych portów lotniczych w Tunezji, Turcji, Egipcie, Libanie, Jordanii i Arabii Saudyjskiej do Europy otrzymali zakaz przewożenia przedmiotów takich jak telefony, laptopy i tablety jako środek zapobiegający potencjalnym zagrożeniom terrorystycznym.

Podjęta inicjatywa oraz skutki ww. zakazu (które został de facto zniesiony w sierpniu 2018 roku), związane z obawami dotyczącymi wpływu ww. na osoby podróżujące w celach osobistych i biznesowych, dały impuls w kierunku firm technologicznych do rozpoczęcia prac nad znalezieniem nowych technologii wykrywania materiałów wybuchowych w urządzeniach elektronicznych.[4]

W ramach inicjatywy wezwano przedsiębiorstwa z całego świata do opracowania nowych systemów umożliwiających wykrywanie materiałów wybuchowych w urządzeniach elektrycznych podczas kontroli bezpieczeństwa na lotniskach lub wewnątrz kabiny.

Chociaż technologie stosowane w przypadku różnych produktów znacznie się różnią, wspólnym celem jest znalezienie szybkiego, przystępnego cenowo i prostego systemu zdolnego do rozpoznania obecności materiału wybuchowego, bez wpływu na obsługę klienta.

Wirtualizacja operacji lotniczych w aspekcie cyberbepieczeństwa

Po katastrofie samolotu Spanair 5022 z 2008 r., która miała miejsce tuż po starcie z pasa startowego, odkryto, że centralny system komputerowy służący do monitorowania problemów technicznych w samolocie został zainfekowany złośliwym oprogramowaniem. Wewnętrzny raport wydany przez linię lotniczą ujawnił, że zainfekowany komputer nie wykrył trzech problemów technicznych z samolotem, które jeśli zostałyby wykryte, mogły uniemożliwić start samolotu. Stwierdzono, że złośliwe oprogramowanie to koń trojański.[5]

Natomiast w 2010 r. FAA opublikowała zawiadomienie wskazujące, że niektóre systemy komputerowe Boeinga 747-8 i 747-8F mogą być podatne na ataki z zewnątrz ze względu na charakter ich łączności.[6]

Porty lotnicze w coraz większym stopniu uskuteczniają przenoszenie części procesów biznesowych do tzw. wirtualnej przestrzeni (operacje w chmurze) w celu usprawnienia wydajności, zmniejszenia początkowych

[4] Airport Technology, UK Lifts ban carrying phones laptops tablets aircraft cabin, https://www.airport-technology.com/news/global-passenger-traffic-aci-report, 31 August 2018.

[5] Komisja Badania Wypadów Lotniczych – CAA Spain, Raport A-032/2008, Accident Involving A Mcdonnell Douglas Dc-9-82 (Md-82) Aircraft, Registration Ec-Hfp, Operated By Spanair, At Madrid-Barajas Airport, On 20 August 2008.

[6] FAA imposes special conditions on 747-8 to prevent hacking, https://www.flightglobal.com/news/articles/faa-imposes-special-conditions-on-747-8-to-prevent-h-337368, 20 January 2010.

inwestycji kapitałowych i zaoferowania elastyczności umożliwiającej dostosowanie się do przepływów pasażerskich. Wiodący dostawcy usług w chmurze dostosowują się do potrzeb branży, ale specjaliści w dziedzinie lotnictwa mają zasadnicze znaczenie, ponieważ wymagane jest prawdziwe zrozumienie środowiska operacyjnego portów lotniczych. Migracja do chmury jest również zadaniem złożonym i każdy negatywny wpływ (opóźnienia, przekroczenie kosztów itp.) na ciągłość działania byłby szkodliwy.

Jednakże trzeba brać uwagę fakt, iż branża lotnicza nie jest bardziej odporna na krytyczne zagrożenia dla bezpieczeństwa cybernetycznego niż jakakolwiek inna. Jest to dość niepokojący fakt, gdy weźmie się pod uwagę potencjalne konsekwencje złośliwego ataku na samolot pełen ludzi. I choć może to zabrzmieć daleko idąco, aby wyobrazić sobie, że wysoce złożone systemy samolotu zostaną zhakowane jednocześnie, napastnik posiadający głęboką wiedzę na temat systemów lotniczych może celowo spowodować poważne problemy z zamierzonymi operacjami samolotu.

Zgodnie z obserwacjami, incydenty związane z bezpieczeństwem cybernetycznym rosną pod względem częstotliwości, skali i złożoności i nie mają granic. Postęp technologiczny i zmiany zachowań ludzi są główną siłą napędową tego trendu i oba te czynniki zmieniają krajobraz ryzyka w wielu sektorach, w tym w transporcie lotniczym.

Ze względu na złożoność systemów lotniczych, na przestrzeni lat wielkość oprogramowania obsługującego te systemy gwałtownie wzrosła. W przypadku, gdy nie są regularnie testowane pod kątem podatności, mogą pojawić się poważne zagrożenia dla bezpieczeństwa. Ponadto zespoły programistów powinny być w stanie skompilować wszystkie znane zagrożenia w celu zbudowania modelu zagrożenia. W ramach tego modelu powinny znajdować się informacje o zagrożeniach, które mają wpływ wyłącznie na produkt lub oprogramowanie znajdujące się w zasięgu ręki. Należy stworzyć model oceny ryzyka w zakresie bezpieczeństwa, aby skutecznie zapobiegać, identyfikować, wykrywać i reagować na wyzwania w zakresie bezpieczeństwa, przed którymi stoi branża lotnicza. Każda awaria to lekcja, której należy się nauczyć.

W najlepszym przypadku względy bezpieczeństwa powinny być uwzględniane na najwcześniejszych etapach projektowania. Zespoły ds. architektury oprogramowania powinny rozważyć potencjalne zagrożenia, przed którymi stają w trakcie cyklu życia oprogramowania, ponieważ pomoże to w zapewnieniu niezawodnego i solidnego oprogramowania.

Coraz ważniejsze staje się posiadanie ugruntowanej polityki bezpieczeństwa cybernetycznego akceptowanej przez wszystkich wiodących producentów oraz akceptowanych standardów awioniki.

W tym scenariuszu istnieje również potrzeba rozważenia istniejących międzynarodowych ram prawnych dla lotnictwa cywilnego z perspektywy

bezpieczeństwa cybernetycznego i określenia, czy potrzebne są dalsze elementy, czy też są one wystarczające.

Ostatnio Konwencja o zwalczaniu bezprawnych czynów odnoszących się do międzynarodowego lotnictwa cywilnego (Konwencja Pekińska) oraz protokół uzupełniający do Konwencji o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi (Protokół Pekiński) wzmocniły globalne ramy prawne dotyczące postępowania w przypadku ataków cybernetycznych na międzynarodowe lotnictwo cywilne.[7]

Bezpieczeństwo cybernetyczne jest priorytetem w ramach globalnej strategii polityki zagranicznej i bezpieczeństwa UE. W rozdziale dotyczącym bezpieczeństwa cybernetycznego w globalnej strategii UE jest mowa o woli UE, aby zwiększyć nacisk na bezpieczeństwo cybernetyczne, wyposażając UE i pomagając państwom członkowskim w ochronie przed zagrożeniami cybernetycznymi przy jednoczesnym zachowaniu otwartej, wolnej i bezpiecznej cyberprzestrzeni.[8]

W 2013 r. Rada z zadowoleniem przyjęła strategię bezpieczeństwa cybernetycznego Unii Europejskiej i podkreśliła, że konieczne i pilne jest dalsze rozwijanie i wdrażanie kompleksowego podejścia do polityki UE w dziedzinie cyberprzestrzeni. W 2014 r. Rada przyjęła ramy polityki obrony cybernetycznej (CDPF) określające obszary priorytetowe służące promowaniu współpracy cywilno-wojskowej i synergii z szerszymi politykami UE w dziedzinie cyberbezpieczeństwa, odpowiednimi instytucjami i agencjami UE, a także z sektorem prywatnym. Obszary te zostały niedawno poddane przeglądowi w celu dostosowania się do zmieniającego się otoczenia cyberprzestrzeni, jak również do inicjatyw UE w zakresie bezpieczeństwa i obrony dotyczących realizacji globalnej strategii UE.[9]

We wrześniu 2017 r. Komisja uruchomiła zaktualizowany pakiet inicjatyw dotyczących bezpieczeństwa cybernetycznego poprzez wspólny komunikat "Odporność, odstraszanie i obrona". Uznano w nim, że wraz z postępującą cyfryzacją i związanymi z tym powiązaniami gospodarki i społeczeństwa przez Internet, krajobraz zagrożeń znacznie się powiększył.

Ponadto grupy państwowe i stowarzyszone z państwem postrzegają obecnie cyberprzestępczość jako broń strategiczną, która niszczy infrastrukturę i dane spowodowane ukierunkowanymi atakami cybernetycznymi. Ataki takie mają obecnie przygnębiającą zdolność do

[7] Future of Air Transport Security, *ICAO Symposium Report*, Montreal 2014.

[8] Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej, Wspólna wizja, wspólne działanie, 2016.

[9] European Defence Agency – Cyber Defence, https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence. 5 September 2017.

doprowadzenia do utraty życia, ponieważ systemy o kluczowym znaczeniu dla bezpieczeństwa, w tym środki transportu, stają się zależne od technologii cyfrowych. Stopień złożoności i skala takich ataków nadal rośnie. Zagrożenia hybrydowe obejmujące ataki cybernetyczne połączone z dezinformacją online zostały wykorzystane do zakłócania procesu decyzyjnego w naszych liberalnych demokracjach. Ponadto przewiduje się, że do 2021 r. cyberprzestępczość będzie nadal rosła i będzie kosztować przedsiębiorstwa na całym świecie ponad 5 trylionów euro rocznie.[10]

Cyberterroryzm nie stanowi odrębnego lub indywidualnego rodzaju terroryzmu ze względu na swoją ideologię. Służy bowiem tym samym celom, którym służą zamachy bombowe, porwania czy branie zakładników, z tą tylko różnicą, że atak ten nie jest widoczny. Cyberterroryzm może przyjmować trzy podstawowe formy. Pierwsza to działania mające na celu włamania, łącznie z nielegalnym pozyskaniem, usuwaniem lub zmianą danych i blokadą serwerów. Prowadzi to do zmian lub uszkodzeń systemów operacyjnych oraz do wielokrotnych połączeń zarówno atakowanego serwera, jak i innych serwerów. Druga formę stanowią wirusy. Są to głównie programy, które działają wbrew woli użytkownika systemu oraz na jego szkodę. Najczęściej stosuje się je, aby niszczyć bazy danych i systemy operacyjne. Kolejna forma to atak konwencjonalny polegający na fizycznym uszkodzeniu elementów systemu komputerowego, serwerów czy infrastruktury telekomunikacyjnej portu lotniczego.

W zależności od sposobu atak tego typu może prowadzić do czasowego paraliżu systemu lub nieodwracalnej utraty danych. Systemy kontroli bezpieczeństwa w portach lotniczych oparte są w większości na zintegrowanych systemach sieciowych, do których jest podłączonych wiele urządzeń, od takich jak: konwencjonalne urządzenia rentgenowskie, urządzenia rentgenowskie wyposażone w automatyczne systemy detekcji materiałów wybuchowych (Explosive Detection Systems – EDS), przez bramki magnetyczne, systemy do skanowania ciała (Full Body Scanners – FBS), specjalistyczne oprogramowanie do projekcji przedmiotów zabronionych w bagażu (Threat Image Projection – TIP) czy na w pełni zautomatyzowanych systemach kontroli bezpieczeństwa bagażu kabinowego kończąc, tzw. systemie scentralizowanego przetwarzania obrazu (Central Image Processing – CIP).

W wyniku daleko idącej komputeryzacji, a co za tym idzie automatyzacji procesów kontroli bezpieczeństwa, każdy pojedynczy sprzęt wykorzystywany dzisiaj do kontroli pasażerów jest komputerem samym w sobie lub w sposób bezpośredni jest podłączony do centralnej jednostki sterującej. W rezultacie w razie próby ataku cybernetycznego na poszczególne elementy systemu może istnieć zagrożenie dopuszczające, że specjalistyczny sprzęt do kontroli

[10] Globalne koszty cyberprzestępczości, Raport Center for Strategic and International Studies, Waszyngton 2017.

bezpieczeństwa pozostanie obojętny na stwierdzone zagrożenie lub zafałszuje wynik kontroli bądź jego kluczowe elementy (jak na przykład mechanizm wyrywkowej kontroli bezpieczeństwa bramek magnetycznych, system TIP czy choćby nawet obraz przekazywany zdalnie poprzez systemy CIP). W tym wypadku bariera między bezpieczeństwem cybernetycznym i fizycznym jest czysto teoretyczna i może stanowi źródło obaw. Dlatego też istotne jest głębsze spojrzenie na wzajemne relacje między bezpieczeństwem cybernetycznym i fizycznym w ekosystemie bezpieczeństwa lotniczego, a także zwrócenie uwagi na rozwój narzędzi świadomości i szkoleń, przede wszystkim dla samych użytkowników systemów bezpieczeństwa.

Rozwój automatyzacji systemów kontroli granicznej

Zautomatyzowany system kontroli granicznej, dzięki któremu podróżni będą poddawani testom przy użyciu awatarów wykrywających kłamstwa, może wkrótce okazać się rzeczywistością. Celem jest przyspieszenie kolejek oraz zwiększenie bezpieczeństwa na zewnętrznych granicach UE. Projekt o nazwie "IBORDERCTRL" ma za zadanie rozwijanie inteligentnych systemów kontroli granicznej, poprzez opracowanie szeregu pytań za pośrednictwem animowanej straży granicznej na ekranie, zanim dotrą oni do granicy, czy to na lądzie, w powietrzu, czy na morzu. Przed dotarciem na lotnisko lub przejście graniczne podróżni będą korzystać z aplikacji online, aby w razie potrzeby załadować zdjęcia swojego paszportu, wizy i dowód posiadania środków finansowych, a następnie za pomocą kamery internetowej odpowiedzieć na pytania komputerowo animowanej straży granicznej, dostosowanej do płci, pochodzenia etnicznego i języka podróżnego.[11]

Technologia mająca na celu "wykrywanie oszustw" przeanalizuje następnie mikro ekspresje podróżnych, aby dowiedzieć się, czy rozmówca mówi prawdę. Po dotarciu do granicy, wszyscy podróżni oznaczeni jako osoby o niskim ryzyku będą kontynuować krótką ponowną ocenę informacji potrzebnych do wjazdu do kraju. Pasażerowie o podwyższonym ryzyku zostaną skierowani do bardziej szczegółowej odprawy z wykorzystaniem danych biometrycznych, która może obejmować przejęcie kontroli granicznej przez straż graniczną z systemu automatycznego.

Ewolucja zagrożeń wewnętrznych w ramach organizacji ekosystemu lotniska

[11] Intelligent Portable Control System Project, https://www.iborderctrl.eu/The-project, 31 August 2019.

Należy przez nie rozumieć zagrożenia spowodowane bezpośrednio szkodliwą działalnością osób pracujących w porcie lotniczym. Może ona mieć charakter sabotażu lub dywersji. Duży problem w tym wypadku stwarza wiedza tych osób oraz ich znajomość infrastruktury portu lotniczego, topografii, a także procesów i procedur ochrony wdrożonych w porcie lotniczym. Wykorzystana w nieodpowiedni sposób może się przyczynić do przeprowadzenia aktu bezprawnej ingerencji w wyniku zastosowania ściśle określonych podatności infrastruktury lotniskowej na zagrożenia. Zagrożenia wewnętrzne mogą mieć charakter typowo przestępczy, jednakże sposób, w jaki są wykonywane, może z powodzeniem służyć do przeprowadzenia aktu terroru z użyciem całego wachlarza środków i materiałów niebezpiecznych.

Grupy terrorystyczne mogą zatrudniać pracowników portów lotniczych w celu ominięcia kontroli bezpieczeństwa - szczególnie pracowników mających bezpośredni dostęp do samolotów. Znane są przypadki, gdy pracownicy przemycali również narkotyki, broń oraz uskuteczniali inne formy przemytu. Tylko jeden radykalny lub niezadowolony pracownik może popełnić czyn, który prowadzi do katastroficznego incydentu, co sprawia, że zajęcie się zagrożeniami wewnętrznymi staje się priorytetem. Porty lotnicze wdrażają własne strategie łagodzenia tego zagrożenia. W większości przypadków działania te obejmowały kontrolę bezpieczeństwa wszystkich lub wybranych pracowników przed wejściem do stref zastrzeżonych. Technologia może również wspierać te wysiłki. Nowe funkcje analityczne wbudowane w systemy wideo i kontroli dostępu mogą stanowić zaawansowane narzędzie nadzoru.

Ewolucja nowych rodzajów zagrożeń wykraczająca poza strefy zastrzeżone lotniska

Zarządzanie zakłóceniami w działalności operacyjnej, które mają wpływ na ciągłość działalności i generowanie przychodów, ma kluczowe znaczenie zarówno dla portów lotniczych, jak i linii lotniczych.

Istnieje znaczna liczba potencjalnych zagrożeń wymierzonych w infrastrukturę portu lotniczego, które to, ze względu na swój rodzaj, mogą się rozciągnąć na bardzo dużą skalę poza granice samego lotniska. Istotnym elementem jest, aby ostrożnie rozróżnić, jakie zagrożenia mają zastosowanie w odniesieniu do poszczególnych obszarów stref ogólnodostępnych lub stref zastrzeżonych lotniska. Biorąc pod uwagę, że największym zagrożeniem dla życia jest atak przeprowadzony w miejscach, w których gromadzi się duża liczba osób, istotne jest, aby zwrócić szczególną uwagę na strefy ogólnodostępne, takie jak: hale odlotowe, poczekalnie, a nawet same punkty kontroli bezpieczeństwa usytuowane w formie scentralizowanych punktów kontroli bezpieczeństwa.

W świetle nowego rodzaju zagrożeń Międzynarodowy Komitet Portów Lotniczych opracował oświadczenie, w którym podsumował zakres działań poszczególnych państw członkowskich odnoszących się do nowych rodzajów zagrożeń. W dokumencie tym Międzynarodowa Rada Portów Lotniczych (ACI) zwróciła uwagę na to, że wejście do terminalu i strefa ogólnodostępna nie różnią się od innych przestrzeni publicznych i podlegają środkom bezpieczeństwa wdrażanym przez władze lokalne. Rada jednocześnie wskazała, że wymiana informacji wywiadowczych to najbardziej praktyczne i realistyczne środki zwalczania terroryzmu, zamiast dodatkowych kontroli bezpieczeństwa

Tabela 1. Lista incydentów terrorystycznych wymierzonych w lotnictwo w latach 2001-2017

Rok	Data	Kraj	Cel ataku	Sprawca ataku	Ofiary	Ranni	Strefy publiczne	Strefy zastrzeżone
2001	11/09/01	USA	Lotnictwo	Al Qaeda	2977	6291+	✗	✓
2002	02/07/02	USA	Lotnictwo	Hesham Mohamed Hadayet	2		✓	✗
2003	04/03/03	Filipiny	Lotnictwo	Abu Sayyaf	21	166	✓	✗
2004	24/08/04	Russia	Lotnictwo	Chechen terrorists	90		✗	✓
2006	09/08/06	W.Brytania	Lotnictwo	Al Qaeda			✓	✗
2006	03/10/06	Turcja	Lotnictwo	Hakan Ekinci			✗	✓
2006	30/12/06	Hiszpania	Lotnictwo	ETA	2	52	✓	✗
2007	03/05/07	Kuba	Lotnictwo	Renegade soldiers	1		✗	✓
2007	30/06/07	W.Brytania	Lotnictwo	Al Qaeda		5	✓	✗
2007	04/09/07	Niemcy	Lotnictwo	Al Qaeda			✓	✗
2009	25/12/09	USA	Lotnictwo	Al Qaeda		3	✗	✓
2010	18/02/10	USA	Lotnictwo	Andrew Joseph Stack	1	13	✓	✗
2010	29/10/10	Yemen	Lotnictwo	Al Qaeda			✗	✓
2011	24/01/11	Rosja	Lotnictwo	Al Qaeda	37	180	✓	✗
2012	29/06/12	Chiny	Lotnictwo	Islamic Terrorists	2	13	✗	✓
2012	18/07/12	Bułgaria	Lotnictwo	Hezbollah	7	34	✓	✗
2012	15/12/12	Pakistan	Lotnictwo	Taliban	4	45	✓	✗
2014	13/02/14	Somalia	Lotnictwo	Al Shabaab	7	19	✓	✗
2014	08/06/14	Pakistan	Lotnictwo	Taliban	14	14	✓	✗
2014	04/07/14	Ukraina	Lotnictwo	Donbas Separatists	298		✓	✗
2015	31/10/15	Egipt	Lotnictwo	IS	224		✗	✓
2015	23/12/15	Turcja	Lotnictwo	Kurdish Freedom Falcons	1		✗	✓
2016	02/02/16	Somalia	Lotnictwo	Al Shabaab		2	✗	✓
2016	05/02/16	Somalia	Lotnictwo	Al Shabaab	3		✓	✗
2016	07/03/16	Somalia	Lotnictwo	Al Shabaab		6	✓	✗
2016	22/03/16	Belgia	Lotnictwo	IS	32	340	✓	✗
2016	28/06/16	Turcja	Lotnictwo	IS	45	239	✓	✗
2016	06/07/16	Yemen	Lotnictwo	Al Qaeda	28	8	✓	✗
2016	17/10/16	Francja	Lotnictwo	Lone wolf - IS		2	✓	✗
2016	21/10/16	W.Brytania	Lotnictwo	Unknown		27	✓	✗
2016	05/11/16	Turcja	Lotnictwo	IS			✓	✗
2016	06/11/16	Bangladesh	Lotnictwo	Lone wolf - IS	1	3	✓	✗
2016	23/12/16	Malta	Lotnictwo	Brigade 93			✗	✓
2017	24/02/17	Bangladesh	Lotnictwo	IS			✓	✗
2017	21/06/17	USA	Lotnictwo	Lone wolf - IS		1	✓	✗
2017	03/10/17	Indie	Lotnictwo	Harkat Ul Mujahideen	1	3	✓	✗
2017	06/10/17	USA	Lotnictwo	Michael C. Estes			✓	✗

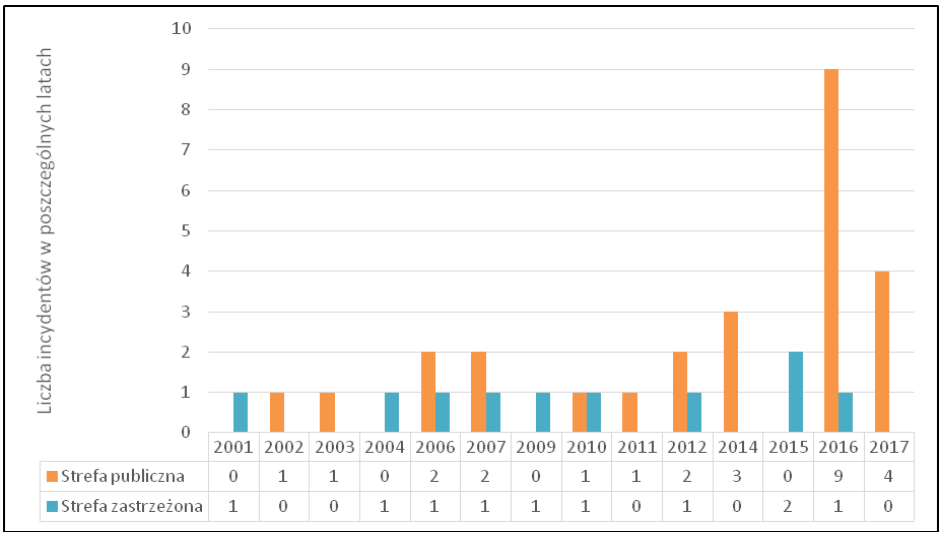
źródło: opracowanie własne

W swoim oświadczeniu ACI wyraźnie podkreśliła, że ewentualne przyjęcie dodatkowych środków bezpieczeństwa, takich jak kontrola osób i towarów wprowadzanych do przestrzeni ogólnodostępnych na lotnisku, może być destrukcyjne i w rzeczywistości tworzyć nowe luki w zabezpieczeniach. Jeśli przesuniemy zgromadzenie pasażerów i gości lotniska na przestrzenie, które nie zostały zaprojektowane do tego celu, to takie środki zasadniczo tylko przesuwają cel, zamiast go chronić.

W ostatecznym rozrachunku pełne zabezpieczenie przestrzeni publicznych przez dodatkowe kontrole bezpieczeństwa byłoby nierealistyczne i nieefektywne. Najlepszy krok w walce przeciwko terroryzmowi to zwiększenie możliwości gromadzenia, koordynacji i dzielenia się informacjami i danymi wywiadowczymi.

Wraz z przyjęciem nowych technologii zainteresowane strony poprawiły swoje reakcje na takie zakłócenia. Szybka ewolucja i penetracja gotowych technologii bezzałogowych, takich jak drony, stanowi jednak poważne wyzwanie. Odległy charakter zakłócenia sprawia, że sprawca jest "nieznany", co dodatkowo zwiększa złożoność zagrożenia.

Są to zagrożenia szczególnego rodzaju, które mają w perspektywie m.in. atak drona wyposażonego w materiały wybuchowe lub inne materiały czy substancje niebezpieczne, takie jak środki chemiczne lub biologiczne. Ataki mogą być wymierzone zarówno w elementy infrastruktury portu lotniczego znajdujące się w strefach ogólnodostępnych (parkingi, hale odlotowe, miejsca składowania towaru), jak i strefach zastrzeżonych (punkty kontroli bezpieczeństwa, płyty postojowe dla samolotów). Zagrożenie to dotyczy także samolotów znajdujących się na drodze kołowania do startu oraz podchodzących do lądowania.



Rys. 1. Wirtualizacja analizy porównawczej incydentów wymierzonych w lotnictwo w latach 2001–2017 z podziałem na strefy ogólnodostępne i zastrzeżone portu lotniczego

źródło: opracowanie własne

Wykorzystanie dronów gwałtownie wzrosło w ostatnich latach, podczas gdy regulacje krajów członkowskich i technologia nadzoru nad ich wykorzystaniem pozostawały w tyle. W rezultacie incydenty, takie jak te, które miały miejsce na lotnisku Gatwick w Londynie w 2018r., spowodowały powszechne zakłócenia i wskazały poważne luki w systemie zabezpieczenia portów lotniczych.

Konkludując wyniki przeprowadzonej analizy, można jednoznacznie stwierdzić, iż skala ataków wymierzonych w strefy publiczne lotnisk sukcesywnie na przestrzeni lat wzrasta. Tym samym staje się poniekąd jednym z głównych celów ataku.

W oparciu o dane, wnioski wyciągnięte w trakcie międzynarodowego forum ds. ochrony lotnictwa cywilnego w ramach panelu roboczego zatytułowanego „Wizja transportu lotniczego 2040 i dalej" zorganizowanego przez *Międzynarodowe Zrzeszenie Przewoźników Powietrznych (IATA*) w czerwcu 2019 roku, została nakreślona przez szerokie grono ekspertów lotniczych wizja przyszłości dot. rozwoju transportu lotniczego, jak i współczesnych zagrożeń. Na jedno z kluczowych pytań postawionych na forum dot. w jaki sposób postrzegana jest wizja zagrożeń w 2040 roku, zebrani uczestnicy niemalże zgodnie lub w podobnym tonie zidentyfikowali następujące obszary wyzwań w kolejności od najbardziej istotnych i alarmujących. W wyniku powyższego wyróżniono:

1) zagrożenie związane z cyberbezpieczeństwem ekosystemów lotniczych w tym zarówno linii jak i portów lotniczych,

2) zwiększoną potrzebę sprawdzania przeszłości w związku z zagrożeniami wewnętrznymi,

3) ataki skierowane na strefy ogólnodostępne infrastruktury portów lotniczych,

4) zagrożenia atakami przy wykorzystaniu środków chemicznych bądź biologicznych zarówno na pokładzie samolotu jak i w ramach infrastruktury lotniskowej,

5) ewolucję metod ukrycia materiałów wybuchowych.[12]

Konkludując, obecni „napastnicy" i ich metody nie znikną, lecz będą podlegać dalszej ewolucji zarówno pod względem technologicznym jak i wyrafinowania prowadzonych działań. W wyniku tego inicjowanie umyślnych zakłóceń w ramach infrastruktury bądź ekosystemu portu lotniczego powinno być uznane za zagrożenie dla lotnictwa cywilnego.

Wyniki własnych badań empirycznych

W referacie przedstawiono wyniki własnych badań empirycznych, przeprowadzonych z najbardziej doświadczonym personelem lotnictwa cywilnego na świecie, m.in. takimi instytucjami jak:

- Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO),
- Międzynarodowe Zrzeszenie Przewoźników Lotniczych (IATA),
- Komisja Europejska (EU COM DG HOME),
- Europejska Organizacja Bezpieczeństwa Lotnictwa (EASA),
- Europejska Konferencja Lotnictwa Cywilnego (ECAC),
- Urząd Lotnictwa Cywilnego (ULC),
- Polska Agencja Żeglugi Powietrznej (PAŻB),
- władze lotniskowe – zarządzających lotniskami (Polska, Francja, Niemcy, Szwecja, Norwegia, Belgia, Holandia, Portugalia, Hiszpania, Austria, Chorwacja, Wielka Brytania, Stany Zjednoczone i Kanada),
- służby odpowiedzialne za zapewnienie bezpieczeństwa i nadzór operacyjny w portach lotniczych (policja, straż graniczna, służba celna, prywatne firmy ochrony).

W badaniach zastosowano dobór ekspercki ze względu na wiedzę i oświadczenie respondentów (118 osób) w zakresie kontroli bezpieczeństwa w lotnictwie cywilnym.

Z przeprowadzonych badań własnych wynika, że kompetencje pracowników ochrony zostały ocenione na poziomie dobrym (59,3 %) – tabela 2.

[12] IATA Report, *Air Transport Security 2040 and Beyond*, Brussels, June 2019.

Tabela2. Kompetencje pracowników ochrony

	Możliwość odpowiedzi	Liczebność	%
1	Bardzo dobry	14	11,9
2	Dobry	70	59,3
3	Dostateczny	30	25,4
4	Niedostateczny	4	3,4

źródło: opracowanie własne

Jednak nie zabrakło ocen określających kompetencje na poziomie dostatecznym (25,%).

Analizując poziom wyszkolenia pracowników ochrony w zakresie czynności kontroli bezpieczeństwa pod względem detekcji przedmiotów zabronionych, wyodrębniono znaczną przewagę respondentów określających wymieniony parametr na poziomie średnim.

Na podstawie rozmów z wybranymi przedstawicielami portów lotniczych wyłania się opinia świadcząca o tym, iż szkoleń nigdy za wiele, w świetle obecnych zagrożeń, a poziom wyszkolenia jest elementem zróżnicowanym – tabela 3.

Tabela 3. Jakość pracy pracowników ochrony w zakresie kontroli bezpieczeństwa

	Możliwość odpowiedzi	Liczebność	%
1	Wysokie	47	39,8
2	Średnie	68	57,6
3	Niskie	3	2,5

źródło: opracowanie własne

W przypadku wyposażenia punktów kontroli bezpieczeństwa w elektroniczne urządzenia wspomagające z wykorzystaniem najnowszych technologii, respondenci określili, że mają one istotne znaczenie do wykrywania potencjalnych zagrożeń (44,1%) oraz bardzo istotne (16,9%).

Tabela 4. Wykorzystanie najnowszej technologii

Możliwość odpowiedzi 1 oznacza ocenę najniższą, a 5 – ocenę najwyższą	Liczebność	%
1	7	5,9
2	7	5,9
3	28	23,7
4	52	44,1
5	20	16,9
Brak odpowiedzi	4	3,4

źródło: opracowanie własne

W kontekście prowadzonych badań dotyczących sposobów zapobiegania zidentyfikowanym zagrożeniom oraz inicjowaniu i wdrażaniu adekwatnych strategii wyodrębniono następujące elementy:

1) konieczność szybszej oceny i reakcji całego sektora lotniczego na występujące zagrożenia, słabość i konsekwencje (lepsza ocena ryzyka i zarządzanie nim),

2) budowanie zaufania transgranicznego i międzyorganizacyjnego,

3) kontynuacja niwelowania różnic i możliwości pomiędzy różnymi poziomami zaawansowania technologicznego w portach lotniczych, poprzez wspieranie wdrażania przystępnych cenowo, ale skutecznych technologii i/lub innowacyjnych programów.

WNIOSKI

Liczba pasażerów w transporcie lotniczym stale rośnie. Z jednej strony wymusza to przyspieszenie procedur kontroli bezpieczeństwa, z drugiej polepszenie jakości tej kontroli.

Lotnictwo komercyjne pozostanie atrakcyjnym celem dla grup bojowników i ekstremistów. Publiczna strona lotnisk - strefa miejska, jest narażona na szereg ataków terrorystycznych.

W świetle tych obiektywnych trudności, należy rozważyć znacznie szersze wykorzystanie cywilnego sektora do wspierania państwowych sił bezpieczeństwa w obronie przed takimi atakami. Korzyści płynące z tego faktu są oczywiste: personel cywilny zazwyczaj kilkakrotnie przewyższa liczbę państwowych sił bezpieczeństwa, większość z nich przechodzi odpowiednie szkolenia, a wielu z nich to byli pracownicy policji i wojska.

W związku z tymi korzyściami oczywiste jest, że prywatny sektor bezpieczeństwa może pomóc zarówno w zapobieganiu atakom terrorystycznym, jak i w radzeniu sobie z ich następstwami (w tym oczyszczanie osób postronnych, udzielanie pierwszej pomocy i ewakuacja ofiar oraz wyeliminowanie dostępu dla osób udzielających pierwszej pomocy).

Jednak wykorzystanie prywatnego sektora bezpieczeństwa w walce z terroryzmem nie jest procesem prostym, który można osiągnąć z dnia na dzień. Rządy w krajach demokratycznych mogą działać jedynie w ramach uprawnień przyznanych im na mocy prawa i nie mogą "wciągnąć" do służby agencji ochrony.

Ponadto prywatni dostawcy usług ochrony mogą nie być chętni do przyjęcia nowej roli w walce z terroryzmem ze względu na znaczne koszty i dodatkową odpowiedzialność, która może być potencjalnie związana z takim krokiem. Wszystkie te kwestie wymagają ram prawnych, aby mogły właściwie funkcjonować

i oczywiście utrzymać właściwą równowagę między bezpieczeństwem a prawami człowieka w społeczeństwie demokratycznym.

W nadchodzących latach otoczenie portów lotniczych ulegnie znacznej przemianie. W połączeniu z rosnącymi oczekiwaniami pasażerów i potrzebą poprawy skuteczności bezpieczeństwa w obliczu zmieniającego się zagrożenia globalnego ten nowy system doprowadzi do zmiany wielu procedur. Bezpieczeństwo stanie się usprawnionym procesem, opartym na współpracy i wymianie danych. Porty lotnicze, które będą chciały zaoferować takie doświadczenie dla pasażerów, będą musiały ponownie przemyśleć swoje procedury ochrony, mając na uwadze takie kwestie, jak:

- wdrożenie technologii umożliwiających poprawę doświadczenia podróżnych,
- wprowadzenie ukierunkowanych działań dotyczących kontroli bezpieczeństwa w zależności od profilu ryzyka pasażera,
- przegląd procesów i procedur ochrony umożliwiających zastosowanie przesiewowych kontroli bezpieczeństwa,
- integracja danych pozwalająca na identyfikację pasażerów na wszystkich etapach ich podróży.

Ochrona zawsze była działalnością związaną z ludźmi, procesami oraz technologią i bardziej niż kiedykolwiek wydaje się, że określony jednolity stopień jej zaawansowania musi być wprowadzony w całym globalnym sektorze lotnictwa, a także w innych wrażliwych sektorach w celu wykrywania zmieniających się zagrożeń. Podczas gdy obecna technologia jest dobra w wykrywaniu materiałów wybuchowych, głównym problemem jest to, że zdolności oraz innowacyjność terrorystów stanowią nadal wyzwanie dla obecnych rozwiązań technologicznych.

Powyższe wnioski potwierdzają jednoznacznie, że hipoteza robocza została zweryfikowana pozytywnie.

BIBLIOGRAFIA

[1] ACI report 6.4% growth in global passenger traffic, https://www.airport-technology.com/news/global-passenger-traffic-aci-report, 17 September 2019.

[2] Airport Technology, UK Lifts ban carrying phones laptops tablets aircraft cabin, 31 August 2018.

[3] European Defence Agency – Cyber Defence, https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence. 5 September 2017.

[4] FAA imposes special conditions on 747-8 to prevent hacking, https://www.flightglobal.com/news/articles/faa-imposes-special-conditions-on-747-8-to-prevent-h-337368, 20 January 2010.

[5] Future of Air Transport Security, *ICAO Symposium Report*, Montreal 2014.

[6] Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej, Wspólna wizja, wspólne działanie, 2016.

[7] Globalne koszty cyberprzestępczości, Center for Strategic and International Studies, Waszyngton 2017.

[8] IATA Report, *Air Transport Security 2040 and Beyond*, Brussels, June 2019.

[9] Intelligent Portable Control System Project, https://www.iborderctrl.eu/The-project, 31 August 2019.

[10] Komisja Badania Wypadów Lotniczych – CAA Spain, Raport A-032/2008, Accident Involving A Mcdonnell Douglas Dc-9-82 (Md-82) Aircraft Operated By Spanair, At Madrid-Barajas Airport, On 20 August 2008.

[11] More Connectivity and Improved Efficiency - 2018 Airline Industry Statistics Released, https://www.iata.org/pressroom/pr/Pages/2019-07-31-01.aspx#__prclt=zTkSP6TZ, 31 July 2019.

[12] Shapiro D., *How did security measures fail in Brussels*, John Jay College of Criminal Justice, March 2016.

SECURITY PROBLEMS OF INTERNATIONAL AIRPORTS

ABSTRACT

The aim of the paper is to present the problems of international airport security. As a result of new types of threats and a significant increase in the number of passengers, new technological solutions are introduced which influence the security of security restricted areas and public areas.

This problem, because of its complexity and unpredictability, still leaves a wide margin for improvement and efficiency.

On the basis of the studies carried out the work hypothesis, that the professional competence of security personnel and the appropriate selection of

electronic assistive devices play an important role in the security of an international airport.

Keywords:
security, terrorism, aviation, new technologies