Tadeusz ZIELIŃSKI
Akademia Sztuki Wojennej

ZAGROŻENIA I PRZECIWDZIAŁANIE BEZZAŁOGOWYM STATKOM POWIETRZNYM W OCHRONIE PORTÓW LOTNICZYCH

STRESZCZENIE

Powszechny dostęp do bezzałogowych statków powietrznych popularnie określanych dronami powoduje, że coraz częściej zdarzają się incydenty z ich udziałem. Zagrożenia generowane przez drony w odniesieniu do infrastruktury krytycznej, w tym portów lotniczych, niezależnie od tego czy powstają w sposób intencjonalny czy nieintencjonalny stwarzają realne niebezpieczeństwo dla funkcjonowania portów lotniczych. Nieautoryzowane wtargnięcie drona w obszar portu lotniczego lub jego świadome wykorzystanie jako narzędzie aktu terrorystycznego mogą być bezpośrednią przyczyną kolizji ze statkiem powietrznym lub spowodować zniszczenie (uszkodzenie) infrastruktury portu lotniczego. Ochrona portu lotniczego przed tego rodzaju zagrożeniami wymaga kompleksowego podejścia obejmującego: wprowadzanie adekwatnych regulacji prawnych, zbudowanie systemu zapobiegania zagrożeniom, utrzymywanie w gotowości zasobów zapewniających wykrywanie, identyfikację i neutralizację zagrożeń generowanych przez drony oraz zbieranie doświadczeń..

Słowa kluczowe:
bezzałogowy statek powietrzny, drony, port lotniczy, systemy antydronowe, zagrożenia

WSTĘP

Na funkcjonowanie portu lotniczego składają się złożone procesy ukierunkowane na realizację przewozów lotniczych (pasażerskich oraz ładunków), których głównym wyznacznikiem jest zapewnienie na każdym etapie wykonania zadania lotniczego bezpieczeństwa zarówno na ziemi jak i w powietrzu. Celowe lub przypadkowe zakłócenie tych procesów może przynieść dla portu

lotniczego duże straty finansowe, jak również spowodować utratę zaufania pasażerów i firm w kwestiach związanych z bezpieczeństwem. Jednym z realnych zagrożeń, które coraz częściej dotyka funkcjonowania portów lotniczych są drony, które pojawiają się zarówno w strefie operacyjnej lotniska jak i jego strefie ogólnodostępnej. Stanowią one poważne zagrożenie dla bezpieczeństwa i mogą spowodować wprowadzenie przez kontrolerów ograniczeń operacyjnych lub zamknięcie lotniska. Z kolei loty dronów w pobliżu innych, niekrytycznych stref lotniska lub otoczenia mogą zakłócić jego rutynowe działanie, ponieważ funkcjonariusze ochrony lotniska, straż graniczna lub funkcjonariusze policji będą zmuszeni do reagowania na takie zdarzenia.

Większość nieintencjonalnych zdarzeń z wykorzystaniem dronów może zostać ograniczona poprzez zastosowanie odpowiednich regulacji prawnych oraz rozpowszechnianie wiedzy na ten temat wśród użytkowników bezzałogowych statków powietrznych (BSP) Tym nie mniej pozostaje w dalszym ciągu grupa zdarzeń, w której drony mogą być użyte celowo (intencjonalnie) z zamiarem dokonania aktu bezprawnej ingerencji lub wyrządzenia szkód w infrastrukturze portu lotniczego. W tego rodzaju przypadkach regulacje prawne będą niewystarczające. Wraz ze wzrostem liczby operacji dronów i postępem technologicznym konieczne stanie się zapewnienie stałych i niezawodnych rozwiązań mających na celu przeciwdziałanie zagrożeniom generowanym przez drony w obszarze portu lotniczego. Jednocześnie, należy zachować balans pomiędzy zminimalizowaniem ryzyka generowanego przez intencjonalne wykorzystanie dronów w sposób niezgodny z prawem a zapewnieniem adekwatnych systemów antydronowych umożliwiających wykrywanie, identyfikację oraz neutralizację dronów. Należy podkreślić, że nie istnieją uniwersalne systemy zapewniające ochronę i obronę portu lotniczego przed zagrożeniami od bezzałogowych statków powietrznych. Każde lotnisko charakteryzuje się unikalnymi właściwościami i jest w różny sposób narażone na zagrożenia wynikające z operowania dronami w sposób niezgodny z regulacjami prawnymi w jego pobliżu. Tym samym, niezbędne jest zastosowanie kompleksowego podejścia uwzględniającego zarówno regulacje prawne jak również rozwiązania technologiczne pozwalające na minimalizowanie ryzyka związanego z zagrożeniami generowanymi przez drony w obszarze funkcjonowania portu lotniczego.

Biorąc powyższe pod uwagę celem przeprowadzonych badań była identyfikacja i klasyfikacja zagrożeń generowanych przez drony w odniesieniu do bezpieczeństwa portu lotniczego oraz określenie obszarów kompleksowego

podejścia do przeciwdziałania tym zagrożeniom. Wyniki badań odpowiadają na dwa kluczowe problemy badawcze sformułowane w postaci następujących pytań: 1) jakie zagrożenia generują użytkownicy dronów dla bezpieczeństwa portu lotniczego? 2) jakie kwestie powinny zostać uwzględnione w kompleksowym przeciwdziałaniu zagrożeniom związanym z użytkowaniem dronów, aby zminimalizować ryzyko dla bezpieczeństwa portu lotniczego?

W celu odpowiedzi na sformułowane problemy badawcze zastosowano teoretyczne metody badawcze obejmujące analizę i krytykę literatury. Pierwsza grupa literatury obejmowała publikacje naukowe odnoszące się do problematyki zastosowań dronów oraz zagrożeń wynikających z ich użytkowania w odniesieniu do bezpieczeństwa infrastruktury krytycznej, w tym portów lotniczych [4, 9, 10, 19, 24]. Druga grupa literatury to dokumenty normatywne w tym polityki instytucji i organizacji międzynarodowych odpowiedzialnych za bezpieczeństwo lotnictwa cywilnego w tym portów lotniczych [6, 7, 20, 22]. W tym kontekście za kluczowe należy uznać opracowania Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego (ang. European Union Aviation Safety Agency, EASA) oraz Międzynarodowej Rady Portów Lotniczych (ang. Airports Council International, ACI). Trzecia grupa literatury obejmowała opracowania think tanków oraz przedsiębiorstw zapewniających rozwiązania w zakresie przeciwdziałania zagrożeniom generowanym przez drony [1-3, 5, 14, 15, 23].

Poprzez zastosowane metody badawcze zidentyfikowano kluczowe zagrożenia generowane przez drony dla bezpieczeństwa portu lotniczego, w tym przede wszystkim: wtargnięcie drona w obszar portu lotniczego, nieautoryzowaną obserwację infrastruktury portu lotniczego z użyciem drona, fizyczne uszkodzenie infrastruktury portu lotniczego, w tym zamach terrorystyczny z użyciem drona, kolizje drona z innym statkiem powietrznym w powietrzu lub na ziemi. Jednocześnie należy podkreślić, iż nie jest to katalog zamknięty potencjalnych zagrożeń. Określono dychotomiczny podział powyższych zagrożeń na: intencjonalne (świadome) oraz nieintencjonalne (wynikające z braku wiedzy oraz bezmyślności użytkowników dronów). Ponadto określono również zagadnienia, które powinny zostać uwzględnione w kompleksowym przeciwdziałaniu zagrożeniom generowanym przez drony dla bezpieczeństwa portu lotniczego. Wśród nich za najbardziej istotne należy uznać: regulacje prawne, zapobieganie, gotowość systemu do minimalizacji ryzyk oraz wykrywanie, identyfikację i neutralizację dronów zagrażających bezpieczeństwu portu lotniczego.

ZAGROŻENIA GENEROWANE PRZEZ BEZZAŁOGOWE STATKI POWIETRZNE

Bezzałogowe statki powietrzne określane powszechnie dronami są statkami powietrznymi, które nie wymagają na pokładzie pilota (załogi), są pilotowane zdalnie lub mogą wykonywać lot w sposób zautomatyzowany (autonomiczny). Rynek dronów obejmuje różnorodne konstrukcje, zarówno duże o maksymalnej masie startowej przekraczającej kilkaset kilogramów po małe, których maksymalna masa startowa wynosi poniżej jednego kilograma. Niezależnie od wielkości i masy, każda z nich użytkowana w niewłaściwy sposób może zagrażać bezpieczeństwu operacji w porcie lotniczym lub w jego pobliżu. Szczególne ryzyko będą stwarzać małe bezzałogowe statki powietrzne (mBSP), szeroko dostępne komercyjnie, które mogą być dodatkowo modyfikowane przez nieodpowiedzialnych użytkowników jako narzędzie aktu bezprawnej ingerencji. Należy zauważyć, że największe zagrożenie dla bezpieczeństwa portów lotniczych stwarzać będą BSP klasy I (do 150 kg masy startowej) bezpośrednio dostępne na rynku, z czego większość nie będzie przekraczała 10 kg maksymalnej masy startowej. Z reguły będą to konstrukcje pionowego startu i lądowania oraz w niewielkim stopniu stałopłaty. Należy założyć, że typowy zasięg komercyjnych mBSP będzie wynosił od jednego do kilkudziesięciu kilometrów, w zależności od typu statku powietrznego. Z kolei zasięg łączności pomiędzy stacją kontroli i bezzałogowym statkiem powietrznym uzależniony będzie od wielu czynników, m.in. środowiska, pasma częstotliwości czy mocy nadajnika. Trzeba zaznaczyć, że komercyjne bezzałogowce będą użytkowały z reguły cywilne pasma częstotliwości w związku z czym będą bardziej podatne na zakłócenia. Typowy zasięg łączności komercyjnych mBSP będzie wynosił od 1 do 10 kilometrów. Istotnym atrybutem mBSP będzie także długotrwałość lotu. Oczywiste jest, że stałopłaty mają w tym względzie przewagę nad pionowzlotami. Rodzaj zastosowanego silnika oraz konstrukcji będą głównymi wyznacznikami długotrwałości lotu bezzałogowców. Należy uznać, że długotrwałość lotu typowych komercyjnych mBSP będzie wynosiła od sześćdziesięciu do dziewięćdziesięciu minut w przypadku samolotów oraz około 30 minut lotu w przypadku statków powietrznych pionowego startu i lądowania. W odniesieniu do pułapu, na którym będą wykonywały zadania komercyjne mBSP należy zauważyć, że będzie on uzależniony od specyfiki zadania oraz rodzaju wykorzystywanych sensorów. Zakłada się, że typowy pułap operacyjny dla komercyjnych mBSP będzie wynosił do 300 m od poziomu gruntu. Również ich prędkość będzie niższa w stosunku do typowych wojskowych konstrukcji i z

reguły wynosi od 30 do 180 km/h w przypadku bezzałogowych samolotów oraz do około 50 km/h w przypadku bezzałogowców pionowego startu i lądowania [12].

Bez wątpienia, o wartości użytkowej (operacyjnej) bezzałogowych statków powietrznych, w tym komercyjnych, decydować będą montowane (przenoszone) sensory i ładunki. Należy zaznaczyć, że masa samych sensorów (ładunków) uzależniona jest od możliwości konstrukcyjnych bezzałogowego statku powietrznego. Przyjmuje się, że w przypadku komercyjnych BSP masa sensorów (ładunków) nie przekracza 10–20% maksymalnej masy startowej statku powietrznego, tym samym z reguły będą to głowice z kamerami o masie do około 5 kg. W przypadku bezzałogowych wielowirnikowych konstrukcji zastosowanie odpowiedniego napędu może zwiększyć masę przenoszonych ładunków do 30–40% maksymalnej masy startowej. W większości przypadków, dostępne na rynku sensory możliwe do zastosowania w komercyjnych mBSP obejmują kamery, zarówno analogowe jak i HD. W mniejszym stopniu są wykorzystywane (ze względu na wysokie ceny i trudności w dostępie) kamery na podczerwień. Niektóre państwa reglamentują otwarty dostęp do tego rodzaju technologii. Na rynku cywilnym dostępne są również inne sensory, w tym kamery wielospektralne, radary z syntetyczną aperturą, kamery stereoskopowe, magnetometry czy urządzenia typu LIDAR, jednakże nie będą one z reguły użytkowane w komercyjnych mBSP. Jednym z trendów, który uwidacznia się również w odniesieniu do komercyjnych mBSP jest możliwość podwieszania uzbrojenia zarówno śmiercionośnego, jak i nieśmiercionośnego. Wówczas mogą one spełniać rolę platform przenoszących uzbrojenie lub stanowić same w sobie kierowane uzbrojenie. Istnieje zatem realne zagrożenie wykorzystania tego rodzaju rozwiązań przez podmioty terrorystyczne.

Przedstawione powyżej atrybuty komercyjnych mBSP (tabela 1) sprawiają, że są one przede wszystkim łatwo dostępne i relatywnie tanie, stąd mogą być wykorzystywane również przez podmioty niepaństwowe, w tym organizacje terrorystyczne, co stwarza realne zagrożenie dla bezpieczeństwa portu lotniczego. Charakterystyczną cechą tych konstrukcji jest ich niewielka masa (1–11 kg) i bardzo duża mobilność w zakresie wykorzystania. Coraz częściej będą pojawiać się konstrukcje kategorii nano, ważące zaledwie kilka lub kilkanaście gramów. Z kolei zastosowanie w produkcji nowoczesnych materiałów spowoduje ich zwiększoną wytrzymałość, a tym samym użyteczność, jak również po-

woduje utrudnienia w zakresie wykrywania takich obiektów, a następnie ich identyfikacji.

Tabela 1. Atrybuty małych bezzałogowych statków powietrznych

Dane	Wartość	Atrybuty
Masa	do 10 kg	– dostępność – niski koszt zakupu – możliwość modyfikacji – gabaryty – materiały – wysokość i prędkość lotu – mobilność – wykrywalność
Systemy startu	wyrzucane z ręki, katapulty, konwencjonalnie	
Konstrukcja	stałopłaty, wielowirnikowce	
Stacja kontroli	laptop, smartfon, tablet	
Zasięg	od 1 do kilkudziesięciu kilometrów	
Zasięg łączności	od 1 do 10 km	
Długotrwałość lotu	ok. 60-90 min, ok. 30 (wielowirnikowce)	
Pułap	do 300 m	
Prędkość	30–180 km/h; do 50 km/h (wielowirnikowce)	
Masa ładunku	Ok. 10–20% MTOW (ok. 5 kg)	

źródło: opracowanie własne

Najbardziej podstawowym ryzykiem związanym z zagrożeniem generowanym przez drony dla bezpieczeństwa portu lotniczego będzie nieuprawniona obserwacja obszaru portu lotniczego i same przeloty dronami w jego obrębie. W ten sposób mogą być zbierane poufne informacje obrazujące pracę i funkcjonowanie portu lotniczego, co może zostać wykorzystane w późniejszym okresie do przeprowadzenia aktu terrorystycznego [9]. Gromadzenie informacji stanowi fundamentalne zagrożenie dla bezpieczeństwa potu lotniczego, ale może być również wstępem do dalszych eskalacji i ataków po zidentyfikowaniu krytycznych elementów infrastruktury portu lotniczego oraz realizowanych tam procesów.

Kolejne zagrożenie związane jest z bezpośrednim wtargnięciem drona w obszar chroniony portu lotniczego. Działanie to może być celowe i świadome związane z aktem terrorystycznym lub kryminogennym. Wówczas stwarza bardzo realne niebezpieczeństwo dla ochrony portu lotniczego [4]. Z drugiej strony może to być akt nieświadomy lub przypadkowy związany z brakiem wiedzy ze strony osoby pilotującej drona, co nie znaczy, że niebezpieczeństwo wystąpienia np. kolizji z samolotem podchodzącym do lądowania lub zagrożenie dla mienia na terenie portu lotniczego jest mniejsze.

Istotnym współcześnie zagrożeniem dla bezpieczeństwa portu lotniczego jest wykorzystanie drona do zbierania informacji o przepustowości połączeń internetowych, a także o lukach w zabezpieczeniach sieciowych na obszarze portu lotniczego, a w konsekwencji jego wykorzystanie do ataku cybernetycznego na infrastrukturę portu lotniczego, co może doprowadzić do jego paraliżu na długie godziny przynoszące realne straty portowi lotniczemu oraz liniom lotniczym [16].

Największe ryzyko dla bezpieczeństwa portu lotniczego niesie ze sobą wykorzystanie drona jako platformy przenoszącej ładunek wybuchowy (profesjonalny lub improwizowany). Pomimo niewielkich gabarytów i stosunkowo niedużego udźwigu rzeczywistego, podwieszenie pod drona nawet kilku granatów lub skonstruowanej domowym sposobem bomby zapalającej może przynieść duże zniszczenia w infrastrukturze portu lotniczego wyłączając go z użytkowania na wiele dni [15].

Przedstawione powyżej przykłady zagrożeń stwarzanych przez drony dla bezpieczeństwa portu lotniczego nie stanowią katalogu zamkniętego. Ważne są również zamiary osób (podmiotów) użytkujących drony w pobliżu portów lotniczych (tabela 2). Można je sklasyfikować na nieintencjonalne oraz intencjonalne. W ramach zachowań nieintencjonalnych można wyróżnić dwie kategorie: zaniedbania oraz rażące zaniedbania. Pierwsza grupa obejmuje osoby bezmyślne, które nie znają lub nie rozumieją obowiązujących przepisów i ograniczeń. W rezultacie latają dronami w obszarach wrażliwych lub zakazanych. Ich postawę można określić jako „bezradną" i nie mającą zamiaru zakłócać funkcjonowania lotnictwa cywilnego. Druga grupa, to osoby nieostrożne, które znają obowiązujące przepisy i ograniczenia, ale naruszają je z własnej winy lub zaniedbania. W rezultacie latają dronami w obszarach wrażliwych lub zakazanych. Osoby te nie mają zamiaru zakłócać funkcjonowania lotnictwa cywilnego, w tym bezpieczeństwa portu lotniczego. Z kolei rażące zaniedbania obejmują działania osób lekkomyślnych, które znają obowiązujące przepisy i ograniczenia, ale celowo nie przestrzegają zasad w celu osiągnięcia osobistych lub zawodowych korzyści. Ich zachowanie można scharakteryzować jako „lekkomyślne", ponieważ zakłócają funkcjonowanie portu lotniczego całkowicie lekceważąc konsekwencje swoich działań [6].

Rażące zaniedbania, to także działania aktywistów/protestujących, którzy niezależnie od tego, czy znają obowiązujące przepisy i ograniczenia lub nie, aktywnie starają się wykorzystywać drony do zakłócania lotnisk i operacji lot-

niczych. Aby zmaksymalizować wpływ, osoby te mogą nawet działać jako grupa. Chociaż ich działania mogą mieć niezamierzone konsekwencje dla bezpieczeństwa portu lotniczego, nie mają zamiaru zagrażać ludzkiemu życiu.

Zachowania intencjonalne obejmują działania przestępcze oraz terrorystyczne prowadzone przez osoby, które niezależnie od tego, czy znają obowiązujące przepisy i ograniczenia lub nie, aktywnie dążą do wykorzystania dronów do ingerencji w bezpieczeństwo i ochronę portu lotniczego. Ponieważ ich działania są celowe i nie mają względu na ludzkie życie i mienie, osoby te należy uważać za osoby motywowane przestępstwem, a nawet terrorystów.

Tabela 2. Klasyfikacja motywacji osób stwarzających zagrożenia dla bezpieczeństwa portu lotniczego z wykorzystaniem dronów

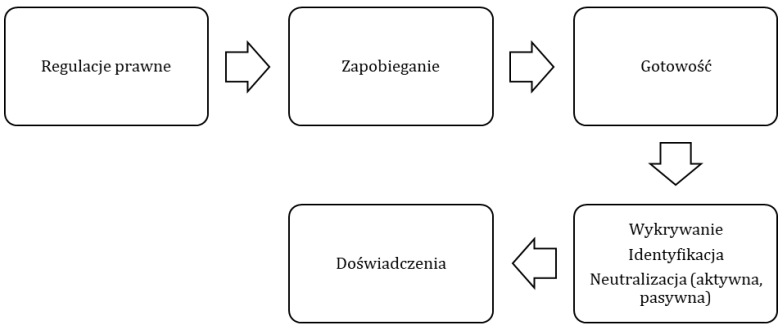
Nieintencjonalne	zaniedbania	osoby bezmyślne	brak znajomości obowiązującego prawa	– kolizje z innymi użytkownikami przestrzeni powietrznej; – wtargnięcie w obszar portu lotniczego – gromadzenie i publikowanie danych – uszkodzenie ciała lub mienia na ziemi
		osoby nieostrożne	znajomość obowiązującego prawa	
	rażące zaniedbania	osoby lekkomyślne	znajomość obowiązującego prawa	
		aktywiści/ protestujący	znajomość/ brak znajomości obowiązującego prawa	
Intencjonalne	motywacja przestępcza/ terrorystyczna	przestępcy i terroryści	znajomość/ brak znajomości obowiązującego prawa – świadome i celowe naruszenie przepisów	– kolizje z innymi użytkownikami przestrzeni powietrznej – wtargnięcie w obszar portu lotniczego – gromadzenie i publikowanie danych – uszkodzenie ciała lub mienia na ziemi – nieautoryzowana obserwacja infrastruktury poru lotniczego – atak cybernetyczny na infrastrukturę portu lotniczego

				– fizyczne uszkodzenie infrastruktury portu lotniczego – zamach terrorystyczny z wykorzystaniem ładunku wybuchowego/środków CBRN

źródło: opracowanie własne na podstawie [6]

KOMPLEKSOWE PODEJŚCIE DO PRZECIWDZIAŁANIA ZAGROŻENIOM GENEROWANYM PRZEZ DRONY DLA BEZPIECZEŃSTWA PORTU LOTNICZEGO

Przeciwdziałanie zagrożeniom generowanym przez drony dla bezpieczeństwa portu lotniczego wymaga kompleksowego podejścia (rysunek 1). Powinno ono obejmować przedsięwzięcia, które są komplementarne względem siebie, a ich realizacja zapewni minimalizowanie ryzyk związanych z operacjami dronów w rejonie lotniska. Działania te mogą zawierać: a) implementację adekwatnych regulacji prawnych; b) wdrażanie rozwiązań zapobiegawczych; c) utrzymywanie systemów przeciwdziałania zagrożeniom w gotowości; d) wykrywanie, identyfikację i neutralizację dronów; e) zbieranie doświadczeń i ich wdrażanie.



Rys. 1. Elementy kompleksowego podejścia
źródło: opracowanie własne

Regulacje prawne

W związku z faktem, iż większość incydentów w rejonie lotniska związanych jest z nieintencjonalnym użytkowaniem dronów, należy spodziewać się, że adekwatne regulacje prawne powinny to ryzyko zminimalizować. Należy podkreślić, że przepisy związane z użytkowaniem dronów są realizowane na poziomie globalnym (Organizacja Międzynarodowego Lotnictwa Cywilnego, ICAO) regionalnym (Agencja UE ds. Bezpieczeństwa Lotniczego) oraz krajowym (w przypadku Polski – Urząd Lotnictwa Cywilnego, ULC). Wdrażane przepisy mają przede wszystkim na celu zapewnienie bezpieczeństwa wszystkim użytkownikom przestrzeni powietrznej, jak również osobom i mieniu znajdującym się na ziemi [20]. Trzeba zauważyć, że aktualne przepisy przyjęte przez Unię Europejską zastępują przepisy krajowe i jest do dobre posunięcie unifikujące operacje realizowane z użyciem dronów. Konieczność posiadania uprawnień przez osoby pilotujące drony (o masie powyżej 250 g) wymaga wykazania się odpowiednim poziomem wiedzy nabytym w trakcie szkolenia i zweryfikowanym podczas egzaminu. Co więcej, użytkownik drona musi zarejestrować się, aby móc wykonywać operacje z wykorzystaniem drona. Już ten nakaz spowoduje, że świadomość użytkowników wzrośnie, w szczególności w odniesieniu do tego, gdzie i na jakich zasadach można latać dronem. Istnieje zatem duże prawdopodobieństwo, że liczba lotów w obrębie portów lotniczych zmaleje lub będą one realizowane w sposób nieingerujący w bezpieczeństwo portu lotniczego [5]. Z kolei konieczność rejestracji użytkownika drona spowoduje, że nie będą oni anonimowi i łatwiej będzie można wyciągać konsekwencje w stosunku do osób, które świadomie naruszają przepisy bezpieczeństwa, w tym w odniesieniu do portów lotniczych.

Wdrażanie rozwiązań zapobiegawczych

Poza regulacjami prawnymi fundamentem kompleksowego podejścia do przeciwdziałania zagrożeniom związanym z użytkowaniem dronów powinny być działania zapobiegawcze, ukierunkowane przede wszystkim na zwiększanie świadomości użytkowników dronów. Powinny to być kampanie informacyjne organizowane przez władzę lotniczą docierające do jak najszerszego kręgu użytkowników dronów. Kolejnym elementem mogą być seminaria i konferencje, w trakcie których będą wyjaśniane zagadnienia wywołujące wątpliwości lub obawy społeczności użytkującej drony. Tylko świadome korzystanie z dronów będzie zapobiegać występowaniu nieintencjonalnych zagrożeń dla bezpieczeństwa portów lotniczych czy sektora lotniczego w ogóle [3]. W tym kontekście istotne jest również egzekwowanie prawa przez właściwe służby państwowe, polegające na identyfikacji osób naruszających przepisy związane z użytkowaniem dronów oraz ewentualną neutralizację zagrożenia

generowanego przez użytkowników dronów. Egzekwowanie prawa w tym obszarze jest możliwe w oparciu o adekwatne regulacje prawne zawarte w wielu aktach prawnych, w tym w ustawie Prawo lotnicze.

Utrzymywanie systemów przeciwdziałania zagrożeniom w gotowości

Opracowanie systemu zapewniającego przeciwdziałanie zagrożeniom generowanym przez drony w odniesieniu do bezpieczeństwa portu lotniczego wymaga zaangażowania wielu służb państwowych. Ponadto, należy zauważyć, że każdy port lotniczy charakteryzuje się indywidualnymi cechami, nie jest więc możliwe opracowanie zunifikowanego systemu zapobiegania. Tym nie mniej, gotowość właściwych służb do przeciwdziałania zagrożeniom w tym obszarze powinna opierać się na doskonaleniu istniejących procedur oraz wdrażaniu istniejących i przełomowych technologii, które pozwolą na minimalizowanie ryzyk [2]. Ważnym elementem tego systemu powinny być ćwiczenia pozwalające na sprawdzenie funkcjonujących procedur w zakresie przeciwdziałania dronom w obszarze portu lotniczego. Jako przykład mogą posłużyć ćwiczenia po kryptonimem Black Dart przeprowadzane przez Stany Zjednoczone od 2002 r. W ramach ćwiczeń agencje rządowe, uczelnie i prywatne spółki testują najnowsze technologie przeznaczone do neutralizacji i zwalczania nieprzyjacielskich dronów. Scenariusze ćwiczenia Black Dart zapewniają realistyczne warunki generowania zagrożeń przez drony, w tym dla bezpieczeństwa infrastruktury krytycznej oraz sposoby przeciwdziałania. Zebrane doświadczenia pozwalają na uaktualnienie istniejących taktyk, technik i procedur w zakresie przeciwdziałania dronom.

Wykrywanie, identyfikacja i neutralizacja dronów

Na wstępie należy zaznaczyć, że nie ma uniwersalnego systemu zapewniającego wykrywanie, identyfikację oraz neutralizację dronów. Tylko połączone metody umożliwią ograniczenie lub pełne oddalenie tego rodzaju ryzyka.

Podstawowa metoda wykrywania dronów jest oparta na technologii radarowej. Radar z jedną lub wieloma antenami służy do jednoczesnego wykrywania i śledzenia wielu obiektów. W ostatnich latach prowadzone są badania w zakresie zastosowań specjalistycznych radarów do detekcji dronów. W porównaniu z innymi technologiami, radar jest w stanie zapewnić wykrywanie dalekiego zasięgu do kilkuset kilometrów, w zależności od wielkości i rodzaju obserwowanego obiektu. Z drugiej strony wyzwaniami związanymi z wykorzy-

staniem radarów są brak automatyzacji i duża zależność od wyszkolenia operatorów radarów. Co więcej, radar jest najdroższym urządzeniem spośród wszystkich dostępnych sensorów do wykrywania dronów i wymaga krajowych licencji na widmo częstotliwości oraz badania kompatybilności środowiskowej [9]. Na lotniskach radary są wykorzystywane do wykrywania dużych obiektów, głównie samolotów poruszających się z dużymi prędkościami, w związku z tym standardowe urządzenia nie będą wykrywały małych, wolno lecących na małej wysokości bezzałogowych statków powietrznych. Innymi słowy, technologie radarowe wymagają rozwoju technologicznego w kierunku wykrywania małych bezzałogowych statków powietrznych, które stanowią istotne zagrożenie dla bezpieczeństwa funkcjonowania portu lotniczego.

Kolejna technologa umożliwiająca wykrywanie dronów oparta jest na skanerach częstotliwości radiowej, w tym źródeł sygnału WiFi wykorzystujących pasywne wykrywanie, śledzenie i identyfikację bezzałogowego statku powietrznego na podstawie sygnatury komunikacyjnej. Skanowanie częstotliwości monitoruje widmo częstotliwości radiowych i wykrywa sygnały, którymi sterowane są drony [1]. Wykorzystują one algorytmy do skanowania znanych częstotliwości radiowych w celu zlokalizowania dronów emitujących fale radiowe niezależnie od pory dnia i warunków atmosferycznych. Jednakże tego rodzaju systemy nie są w stanie wykryć dronów, które są wstępnie zaprogramowane lub działają w pełni autonomicznie [11]. Podobnie wykrywanie dronów w środowisku dużej emisji częstotliwości jest utrudnione, szczególnie na odległościach powyżej 100 m. Wykrywanie staje się również znacznie trudniejsze w obszarach o dużym zaludnieniu, ponieważ widmo staje się głośniejsze i bardziej zatłoczone.

Jedną z metod detekcji dronów jest wykrywanie akustyczne. Silniki drona lub jego śmigła emitują charakterystyczny wzór dźwiękowy, który można wykryć i wykorzystać do pozycjonowania i klasyfikacji dronów za pomocą czujników akustycznych. Zwykle mikrofon wykrywa dźwięk wytwarzany przez drona i oblicza jego lokalizację. Odpowiednie algorytmy są w stanie identyfikować po dźwięku konkretny typ drona, a nawet rozróżniać pomiędzy dronami autoryzowanymi a nieautoryzowanymi. W większości przypadków czujniki akustyczne mają krótki zasięg wykrywania, poniżej 300 m oraz podlegają ograniczeniom interferencji z innym hałasem słyszalnym, co jest dość znaczące w okolicach lotnisk, gdzie hałas jest ogromny i nakłada się na siebie [18]. Ponadto, czujniki akustyczne opierają się na bazie danych dźwięków wcześniej zidenty-

fikowanych dronów i nie będą reagowały na dźwięki, które do tej pory nie znalazły się w bibliotece danych.

Powszechną metodą wykrywania dornów jest detekcja optyczna polegająca na wykorzystaniu kamer wideo i algorytmów komputerowych do wykrywania dronów. Nie jest to zwykle główne źródło wykrywania, czujniki elektrooptyczne wykorzystują sygnaturę wizualną do wykrywania dronów, a czujniki podczerwieni wykorzystują sygnaturę cieplną. Zaawansowane systemy kamer dostarczają obrazy jako dowody sądowe. Często są wyposażone w funkcję dużego zoomu, aby pokazać małe obiekty z dużej odległości; mają jednak ograniczenia związane z zasięgiem. Trwają również prace nad metodami wykrywania drona i jego trajektorii za pomocą sygnałów ruchu, znaków wizualnych i deskryptorów kształtu. Połączone wykorzystanie sieci neuronowych i algorytmów głębokiego uczenia z danymi optycznymi, mogą zapewnić znaczące wsparcie i zaawansowaną inteligencję systemowi wykrywania bezzałogowych statków powietrznych. Wykrywanie i identyfikacja dronów metodami wizualnymi jest także możliwe poprzez zastosowanie obrazów hiperspektralnych. Dzięki nim możliwa jest dokładna lokalizacja i identyfikacja dronów. Tym nie mniej, mogą pojawić się błędy polegające na podobieństwach w ruchu dronów oraz ptaków.

W odróżnieniu od czujników optycznych sensory termiczne wykorzystują niewidzialne widmo elektromagnetyczne, stąd kamery termowizyjne mogą śledzić promieniowanie podczerwone emitowane przez obiekty latające w postaci ciepła. Wykorzystują one zakres widma elektromagnetycznego w dalekiej podczerwieni, o długości fali 9–14 μm [17]. Dlatego kamery termowizyjne mogą znaleźć zastosowanie do wykrywania dronów w środowiskach, w których nie będzie można stosować pozostałych urządzeń optoelektronicznych. Podobne działania podjęto z wykorzystaniem czujników LIDAR – przyniosły one dobrą dokładność wykrywania dronów w zasięgu kilkuset metrów. Pomimo zalet czujników na podczerwień i LIDAR nie mogą one identyfikować jednoznacznie dronów ponieważ przechwycone sygnatury mają raczej niska rozdzielczość. Zasadniczo, w systemach detekcji stosuje się kombinację kamer, które przechwytują widzialne i niewidzialne długości fal, aby realizować obserwację w ciągu dnia i nocy. Ten sposób detekcji trudno jest stosować samodzielnie dlatego łączony jest z wykorzystaniem radarów i skanowaniem częstotliwości, jako dodatkowe narzędzie do wykrywania, weryfikacji i analizy w odniesieniu do dronów.

Reasumując, przyjęcie pojedynczej technologii do wykrywania i identyfikacji dronów na lotniskach nie zapewni pożądanej świadomości sytuacyjnej. Jako standard należy stosować różnorodne metody detekcji i identyfikacji bezzałogowych statków powietrznych, szczególnie w obszarze złożonego środowiska portu lotniczego. W przyszłości do wykrywania dronów będą wykorzystywane również inne drony. Jednakże w tym obszarze niezbędne jest wdrożenie systemów zarządzania ruchem bezzałogowych statków powietrznych oraz wymagań dotyczących zdalnej identyfikacji dronów, co umożliwi służbom odpowiedzialnym za zarządzanie przestrzenią powietrzną segregowanie dronów na autoryzowane i nieautoryzowane [22, 13].

Aktualnie na rynku funkcjonuje wiele rozwiązań służących do ograniczania zagrożeń generowanych przez drony użytkowane w nieautoryzowany sposób. Należy podkreślić, że przyjęte metody przeciwdziałania powinny być zgodne z obowiązującym prawem i adekwatne do ryzyka. Dotyczy to również kwestii ochrony portu lotniczego przed zagrożeniami generowanymi przez bezzałogowe statki powietrzne. Jedną z podstawowych metod, w odniesieniu do zagrożeń generowanych przez komercyjne drony wykorzystujące sygnał GPS, będą działania zapobiegawcze polegające na zaimplementowaniu ograniczeń w oprogramowanie dronów, takie jak geofencing. Jego istotą jest wymuszenie, aby drony nie miały możliwości zbliżania się do lotnisk lub innych stref o ograniczonych lub zakazanym dostępie. Są to pewnego rodzaju wirtualne ogrodzenia wokół portów lotniczych uniemożliwiające wtargnięcie drona w ten obszar. Parametry danej strefy są zapisane w oprogramowaniu drona lub mogą być generowane dynamicznie w trakcie lotu [19].

Kolejne technologie służące do neutralizacji dronów obejmują działania elektroniczne i kinetyczne. Zasadniczo, działania elektroniczne bazują na przechwytywaniu lub zagłuszaniu sygnału emitowanego przez drony. Jednym z podstawowych sposobów jest zagłuszanie częstotliwości radiowych polegające na celowym wykorzystaniu transmisji radiowej w celu zablokowania sygnałów i zakłóceniu komunikacji pomiędzy operatorem sterującym dronem ze stacji kontroli a bezzałogowym statkiem powietrznym. Do tego celu przeznaczone są urządzenia stacjonarne (np. montowane na budynkach) lub mobilne (np. przenośne karabiny), które przesyłają dużą ilość energii w kierunku drona tłumiąc sygnał (częstotliwość radiową) przesyłany ze stacji kontroli do drona [14]. W konsekwencji, w zależności od konstrukcji drona: a) wykonuje on kontrolowane lądowanie w swojej aktualnej lokalizacji; b) dron powraca do lokalizacji

wcześniej zdefiniowanej przez użytkownika; c) dron spada w niekontrolowany sposób na ziemię; d) dron odlatuje w losowym niekontrolowanym kierunku. Kolejną opcją jest zagłuszanie sygnału GPS, jeśli dron korzysta z systemów nawigacyjnych opartych na GPS. Oczywiste jest, że większym wyzwaniem będzie zagłuszenie sygnału opartego na łączu satelitarnym niż radiowym, tym nie mniej zasada jest ta sama – do drona wysyłany jest nowy silniejszy sygnał, zastępujący komunikację GPS, którą dron wykorzystuje do nawigacji, co utrudnia sterowanie dronem i uniemożliwia działanie funkcji powrotu do zdefiniowanej lokalizacji [21]. Trzecia opcja opiera się na manipulowaniu protokołem przez osoby, które chcą przejąć kontrolę nad sterowaniem dronem podszywając się pod pilota. W celu zmylenia drona, instrukcje sygnałowe są emitowane w taki sposób, aby zmanipulowany sygnał był postrzegany jako prawdziwy – w ten sposób zostaje przejęta kontrola nad dronem.

Działania kinetyczne obejmują fizyczne aktywności skierowane przeciwko dronom zagrażającym bezpieczeństwu portów lotniczych. Szeroko rozpowszechnioną metodą w tym obszarze jest wykorzystanie siatek do przechwycenia drona [10]. Są one montowane na bezzałogowym statku powietrznym, który wykonuje lot w kierunku nieautoryzowanego drona celem jego schwytania. Tego rodzaju systemy są wykorzystywane na krótkich dystansach i są skuteczne gdy przechwytywany dron porusza się z małą prędkością i nie manewruje. Inną z metod przechwytywania są wyszkolone ptaki drapieżne, które traktują nieautoryzowany dron jako ofiarę [23]. Są one wyposażone w sprzęt ochronny, który służy do atakowania i schwytania drona, który wtargnął w obszar o ograniczonym dostępie. Jednakże ten sposób ma swoje ograniczenia, gdyż ptaki również mogą stwarzać niebezpieczeństwo kolizji ze startującymi lub lądującymi samolotami.

Odrębną grupę metod kinetycznych stanowią te oparte na wykorzystaniu energii elektromagnetycznej o dużej mocy. Wykorzystanie impulsów elektromagnetycznych o dużej mocy lub precyzyjnej broni laserowej pozwala na fizyczne zniszczenie (zestrzelenie) drona poprzez zneutralizowanie jego obwodów elektronicznych [8, 24]. Trzeba również pamiętać, że opcje zastrzelenia drona w obszarze portu lotniczego nie zawsze będą możliwe ze względu na ryzyko niekontrolowanego rozbicia się drona, szczególnie w obszarach kongestii. Stąd, tego rodzaju metody mogą być zakazane ze względów bezpieczeństwa.

Zbieranie doświadczeń i ich wdrażanie

Przedstawione powyżej elementy kompleksowego podejścia do przeciwdziałania zagrożeniom generowanym przez drony dla bezpieczeństwa portu lotniczego będą skuteczne jeśli zostanie wdrożona w ramach konkretnego portu lotniczego procedura zbierania doświadczeń, które następnie znajdą swoje odzwierciedlenie we wdrażanych procedurach oraz taktykach i technikach niwelowania zagrożeń generowanych przez drony [7]. Niezależnie od jakości funkcjonowania poszczególnych elementów, kwestia zbierania i opracowywania doświadczeń powinna być kluczowa, tylko w taki sposób będzie można realnie poprawiać błędy i wdrażać nowe rozwiązania proceduralne i technologiczne.

PODSUMOWANIE

Należy założyć, że częstotliwość, złożoność i dotkliwość incydentów związanych z nieautoryzowanym użyciem dronów w obrębie portów lotniczych będzie gwałtownie wzrastać, ponieważ liczba operacji tego rodzaju statków powietrznych wzrasta drastycznie. Zarówno ich intencjonalne, jak i nieintencjonalne użytkowanie w obszarze portu lotnicze stwarza realne zagrożenie dla powietrznych i naziemnych operacji wykonywanych w porcie lotniczym. Stąd, niezbędne są metody i środki zapobiegania tego rodzaju ryzykom. Pomimo tego, że poszczególne porty lotnicze różnią się cechami konstrukcyjnymi oraz rozmiarami, to mają podobne wymagania w odniesieniu do zapewnienia bezpieczeństwa w zakresie wykrywania, identyfikacji i neutralizacji nieautoryzowanych dronów. W tym kontekście ważne są działania zapobiegawcze, jak zastosowanie metody geofencingu przez producentów dronów, która sama w sobie stanowi element zabezpieczenia dla portów lotniczych. Jednocześnie komplementarne względem siebie stosowanie metod wykrywania i identyfikacji zapewni realną ochronę portów lotniczych przed zagrożeniami generowanymi przez drony.

Z kolei w odniesieniu do neutralizacji zagrożenia generowanego przez drony dla bezpieczeństwa portu lotniczego warto podkreślić, że nie ma jednej skutecznej metody, która znajdzie skuteczne zastosowanie w ochronie portu lotniczego. Podobnie jak w przypadku wykrywania i identyfikacji tylko wzajemnie uzupełniające się metody przeciwdziałania będą skuteczne w minimalizowaniu zagrożeń generowanych przez drony. Niniejszy wydruk jest przykładem formatowania tekstu na stronie i stosowania właściwego kroju i

rozmiaru czcionki. Niniejszy wydruk jest przykładem formatowania tekstu na stronie i stosowania właściwego kroju i rozmiaru czcionki.

BIBLIOGRAFIA

[1] *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Joint Air Power Competence Centre, Kalkar 2021, https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf, [dostęp 6 kwietnia 2022].

[2] *Airport Response to Unmanned Aircraft System (UAS) Threats*, Program for Applied Research in Airport Security, National Safe Skies Alliance, September 2021, https://www.sskies.org/images/uploads/subpage/PARAS_0031.ResponsetoUASThreats_.FinalReport_.pdf, [dostęp 6 kwietnia 2022].

[3] *Blue Ribbon Task Force on UAS Mitigation at Airports*, Final Report 2019, https://uasmitigationatairports.org/wp-content/uploads/2019/10/BRTF-Report2019.pdf, [dostęp 6 kwietnia 2022].

[4] Crino S., Dreby C., D*rone Attacks Against Critical Infrastructure: A Real and Present Threat*, Issue Brief, Atlantic Council 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/05/DRONE-ATTACK-0420-WEB.pdf, [dostęp 6 kwietnia 2022].

[5] *Drone disruption at airports. A risk mitigation and insurance response*, Airport Risk Community 2019, https://www.wtwco.com/-/media/WTW/Insights/2019/07/drone-disruption-at-airports-a-risk-mitigation-and-insurance-response.pdf?modified=20190731151924, [dostęp 6 kwietnia 2022].

[6] *Drone Incident at Aerodromes. Part 1: The challenge of unauthorised drones in the surroundings of aerodromes*, European Union Aviation Safety Agency 2021, https://www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf, [dostęp 6 kwietnia 2022].

[7] *Drones Policy Paper*, Airports Council International 2018, https://aci.aero/wp-

content/uploads/2022/04/ACIPolicyPaper_Drones_2018-1.pdf, [dostęp 6 kwietnia 2022].

[8] Looze D., Plotnikov M., Wicks R., *Current Counter-Drone Technology Solutions to Shield Airports and Approach and Departure Corridors*, University of Massachusetts 2016, https://rosap.ntl.bts.gov/view/dot/35012, [dostęp 6 kwietnia 2022].

[9] Lykou G., Moustakas D., Gritzalis D., *Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies*, "Sensors" 2020, 20(12), 3537, s. 1-40, [https://doi.org/10.3390/s20123537].

[10] Milić A., Radovanović M., Petrovski A., *Protection of critical Infrastructure Facilities Against Drone Attacks Using Drones*, VII International Scientific Professional Conference Security and Crisis Management – Theory and Practise (SeCMan). Safety for the Future, Macedonia, Belgrad 2021, s. 286-293.

[11] Nguyen P., Truong H., Ravindranathan M. i in. *Drone presence detection by identifying physical signatures in the drone'rf communication*, Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, Niagara Falls, NY, USA, 19–23 June 2017, s. 211–224.

[12] Patterson D.R., *Defeating the Threat of Small Unmanned Aerial Systems*, "Air and Space Power Journal", Spring 2017, s. 15-25, https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-2/2017_2_03_patterson_s_eng.pdf, [dostęp 6 kwietnia 2022].

[13] Pledger T.G., *The Role of Drones in Future Terrorist Attacks*, Land Warfare Paper 137, The Association of the United States Army, February 2021, https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf, [dostęp 6 kwietnia 2022].

[14] *Protecting Against the Threat of Unmanned Aircraft Systems (UAS)*, Interagency Security Committee 2020, https://www.cisa.gov/publication/protecting-against-threat-unmanned-aircraft-systems, [dostęp 6 kwietnia 2022].

[15] *Protecting Critical Infrastructure from Drones*, Echodyne, https://www.echodyne.com/media/53pmmxwm/ech_protecting-critical-infrastructure-from-drones_19s26.pdf, [dostęp 6 kwietnia 2022].

[16] Pyrgies J., The UAVs *Threat to Airport Security: Risk Analysis and Mitigation*, "Journal of Airline and Airport Management" 2019, 9(2), s. 63-96, [https://doi.org/10.3926/jairm.127].

[17] Samaras S., Diamantidou E., Ataloglou D. i in., *Deep Learning on Multi Sensor Data for Counter UAV Applications – A Systematic Review*, "Sensors" 2019, 19, 4837, s. 1-35, [https://doi.org/10.3390/s19224837].

[18] Sedunov A., Sutin A., Sedunov N., i in., *Passive acoustic system for tracking low-flying aircraft*, "IET Radar, Sonar & Navigation" 2016, 10, s. 1561–1568, [https://doi.org/10.1049/iet-rsn.2016.0159].

[19] Stevens M.N., Atkins E.M., *Geofencing in Immediate Reaches Airspace for Unmanned Aircraft System Traffic Management*, AIAA Sci Tech Forum, 2018, s. 1-11, [https://doi.org/10.2514/6.2018-2140].

[20] *The European Plan for Aviation Safety (EPAS 2020-2024)*, European Union Aviation Safety Agency 2019, https://www.easa.europa.eu/sites/default/files/dfu/EPAS_2020-2024.pdf, [dostęp 6 kwietnia 2022].

[21] Tippenhauer N., Pöpper C., Rasmussen K., Capkun S., *On the requirements for successful GPS spoofing attacks*, Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011, s. 75–86, [https://doi.org/10.1145/2046707.2046719].

[22] *Unmanned Aircraft System Traffic Management (UTM)*, Federal Aviation Administration, https://www.faa.gov/uas/research_development/traffic_management/, [dostęp 6 kwietnia 2022].

[23] *White Paper: Countering the drone threats to international airports*, Dynamite Global Strategies 2019, https://usdgs.com/wp-content/uploads/2019/09/Whitepaper-Countering-the-Drone-Threat-to-International-Airports.pdf, [dostęp 6 kwietnia 2022].

[24] Zhang X., Kusrini K., *Autonomous long-range drone detection system for critical infrastructure safety*, "Multimedia Tools and Applications" 2021, 80, s. 23723–23743, [https://doi.org/10.1007/s11042-020-10231-x].

THREATS AND COUNTERING UNMANNED AIRCRAFT IN SAFETY OF AIRPORTS

ABSTRACT

The common access to unmanned aircraft, popularly referred to as drones, causes more and more incidents involving this kind of aircraft. Threats generated by drones in relation to critical infrastructure, including airports, regardless of whether they arise intentionally or unintentionally, pose a real threat to the functioning of airports. Unauthorized drone intrusion into the airport area or its deliberate use as a tool of a terrorist act may be a direct cause of a collision with an aircraft or destruction (damage) to airport infrastructure. Protecting an airport against such threats requires a comprehensive approach including: introducing adequate legal regulations, building a threat prevention system, maintaining readiness of resources to detect, identifying and neutralizing threats generated by drones, and gathering lessons learned.