Zeszyty Naukowe SGSP 2022, Nr 83, s. 163–174
ISSN: 0239-5223; e-ISSN: 2720-0779
Creative Commons Attribution 4.0 International License (CC-BY)
DOI: 10.5604/01.3001.0016.0230

dr hab. Grzegorz Pietrek
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
e-mail: grzegorz.pietrek@uph.edu.pl
ORCID: 0000-0003-2660-8025

dr Michalina Pietrek
Akademia Pomorska w Słupsku
e-mail: michalina.pietrek@apsl.edu.pl
ORCID: 0000-0001-7681-4260

BEZZAŁOGOWE STATKI POWIETRZNE JAKO ZAGROŻENIE DLA INFRASTRUKTURY KRYTYCZNEJ PAŃSTWA

Abstrakt

Rozwój różnego rodzaju zagrożeń jest oczywistą konsekwencją wzrostu zaawansowania technicznego. Podział zagrożeń dla ludzi, mienia i środowiska jest różnorodny. Wśród różnych definicji, kryteriów i pojęć znajdują się także takie, które odnoszą się do bezpieczeństwa infrastruktury krytycznej. Po przeanalizowaniu dostępnej literatury można dojść do wniosku, że jednym z zagrożeń, jakie pojawiło się stosunkowo niedawno, a wydaje się być istotnym i „rozwojowym", jest zagrożenie ze strony bezzałogowych statków powietrznych, powszechnie zwanych dronami.
Bezzałogowy statek powietrzny (z ang. *Unmanned Aerial Vehicle*), w swej najprostszej definicji, jest maszyną, która nie wymaga do lotu załogi obecnej na pokładzie, nie ma możliwości zabierania pasażerów i jest pilotowana zdalnie lub wykonuje lot autonomicznie. W rzeczywistości sam statek powietrzny potrzebuje do działania dodatkowych zasobów i urządzeń. Urządzenia te wzajemnie się komunikują i umożliwiają statkowi wykonanie powierzonego mu zadania. W poniższym artykule autorzy mają zamiar osiągnąć cel badań w postaci analizy poziomu zagrożeń dla infrastruktury krytycznej państwa generowanych przez bezzałogowe statki powietrzne.

Słowa kluczowe: infrastruktura krytyczna, zarządzanie bezpieczeństwem, drony, zagrożenie

UNMANNED AERIAL VEHICLE AS A THREAT TO CRITICAL STATE INFRASTRUCTURE

Abstract

The development of various types of threats is an obvious consequence of the increase in technical advancement. The division of threats to people, property and the environment is diverse. In this maze of various definitions, criteria and concepts, we also find those that relate to the security of critical infrastructure. An analysis of the available literature indicates that one of the threats that appeared relatively recently, and seems to be significant and "developmental" in nature, is the threat posed by "unmanned aerial vehicles", commonly known as drones. An Unmanned Aerial Vehicle, in its simplest

Creative Commons Attribution 4.0 International License (CC-BY)

definition, is a machine that does not require an on-board crew for flight, cannot pick up passengers and is remotely piloted or autonomously flown. In fact, the aircraft itself requires additional resources and equipment to operate. These devices communicate with each other and enable the ship to perform its assigned task. In the article below, the authors intend to achieve the research goal of analyzing the level of threats to the state's critical infrastructure generated by unmanned aerial vehicles.

Keywords: critical infrastructure, security management, drones, danger

1. Wprowadzenie

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) (opracowany zgodnie z art. 5b ust. 1 ustawy o zarządzaniu kryzysowym [1]) to dokument, którego zadaniem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. NPOIK określa zasady ochrony infrastruktury krytycznej (IK) oraz współpracy właścicieli IK z administracją publiczną. Jest to dokument nowatorski i wyjątkowy. Jego wyjątkowość polega m.in. na bezsankcyjnym, opartym na zaufaniu i współpracy administracji publicznej z właścicielami i posiadaczami obiektów IK podejściu do ochrony infrastruktury krytycznej. Treść programu wynika bezpośrednio z zapisów ustawy o zarządzaniu kryzysowym i zawartej w niej definicji infrastruktury krytycznej, która pozwala ocenić, które obiekty, urządzenia, instalacje i usługi są kluczowe dla bezpieczeństwa państwa i jego obywateli, a także służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. NPOIK określa narodowe priorytety oraz standardy w zakresie ochrony tychże, w zakresie odpowiedzialności administracji rządowej, samorządowej oraz służb powołanych do zapewnienia bezpieczeństwa narodowego, a przy ich ustalaniu kluczowym kryterium jest ich znaczenie dla niezakłóconego funkcjonowania państwa oraz bezpieczeństwa obywateli. Celem Narodowego Programu Ochrony Infrastruktury Krytycznej jest stworzenie warunków do poprawy bezpieczeństwa IK, w szczególności w zakresie: (1) zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej; (2) przygotowania na sytuacje kryzysowe, które mogą niekorzystnie wpłynąć na infrastrukturę krytyczną; (3) reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej; (4) odtwarzania infrastruktury krytycznej [2].

W załączniku do Programu określono także kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej[1]. Wraz z jednolitym wykazem infrastruktury krytycznej kryteria te zostały opracowane i zaktualizowane przez Rządowe Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnych za poszczególne systemy. Warto dostrzec, że autorzy dokumentu dokonali

[1] Jest to dokument zawierający informacje niejawne, zgodnie z przepisami ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167).

także identyfikacji słabości procedury nakładania na operatorów infrastruktury krytycznej obowiązków w drodze ustaw czy rozporządzeń ze względu na realny brak możliwości prowadzenia audytu i kontroli ich realizacji [3].

2. Materiały i metody

Obszarem problemowym zakreślonym w artykule są zidentyfikowane zagrożenia dla funkcjonowania infrastruktury krytycznej państwa, a w tym szczególnie drony (bezzałogowe statki powietrzne). Na potrzeby pracy określony został cel badań w brzmieniu: analiza poziomu zagrożeń dla infrastruktury krytycznej państwa generowanych przez bezzałogowe statki powietrzne. W kolejnym etapie określono problem badawczy w brzmieniu: jaki jest poziom zidentyfikowanego zagrożenia dla funkcjonowania infrastruktury krytycznej państwa ze strony dronów? Jako hipotezę badawczą przyjęto zdanie: Zakłada się, że zagrożenia ze strony dronów są określane jako wysokie i mogą powodować poważne zakłócenia w funkcjonowaniu infrastruktury krytycznej państwa. Dla realizacji nakreślonego celu, rozwiązania problemu oraz zweryfikowania hipotezy badawczej autorzy posłużyli się głównie następującymi metodami teoretycznymi: analiza literatury przedmiotu, analiza aktów prawnych, synteza, analiza (indukcyjna i dedukcyjna), abstrahowanie, porównanie oraz wnioskowanie. Wnioskowanie przeprowadzono w oparciu o analizę SWOT, metodę z grupy zarządzania strategicznego. Autorzy przyjęli, że wnioski można będzie także wysnuć z analizy dostępnych raportów krajowych oraz zagranicznych, a także z dokumentów, takich jak np. Narodowy Program Ochrony Infrastruktury Krytycznej.

3. Wyniki i dyskusja

Głównym zadaniem Narodowego Programu Ochrony Infrastruktury Krytycznej jest „stworzenie warunków do poprawy bezpieczeństwa IK. Wraz z innymi dokumentami programowymi składa się on na cel nadrzędny – podniesienie bezpieczeństwa Rzeczypospolitej Polskiej" – w tym zakresie dokument nie różni się od edycji poprzedniej. Znaczne różnice ilościowe występują jednak na etapie formułowania celów pośrednich (szczegółowych). Cele te przewidują: zdobycie określonego poziomu świadomości, wiedzy i kompetencji wszystkich uczestników Programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów i metod jej ochrony; wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach; wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony IK; budowa partnerstwa między uczestnikami procesu ochrony IK; wprowadzenie mechanizmów wymiany i ochrony informacji przekazywanych między uczestnikami procesu ochrony IK [3].

Creative Commons Attribution 4.0 International License (CC-BY)

Zakłada się, że „zwiększenie skuteczności ochrony IK może nastąpić jedynie przez działania jej operatorów wspieranych przez możliwości i potencjał administracji publicznej" [3]. Niestety, bezsankcyjność wiąże się także z brakiem wsparcia finansowego operatorów infrastruktury krytycznej, co przedstawione jest jako czynnik równowagi pomiędzy „władczym oddziaływaniem państwa, a wydatkami niezbędnymi do poprawy bezpieczeństwa IK". Przypomniano tym samym, iż „(...) ustawa o zarządzaniu kryzysowym nie przewiduje sankcji za niedopełnienie obowiązków w niej określonych, jak również nie przewiduje wsparcia budżetowego operatorów IK" oraz zaprezentowano katalog zasad ujętych jako wytyczne dla realizowania celów Programu przez jego odbiorców. Wśród nich jako najważniejsze filary wskazano: współodpowiedzialność rozumianą „(...) jako wspólne (zbiorowe) dążenie do poprawy bezpieczeństwa IK wynikające ze świadomości jej znaczenia dla funkcjonowania zarówno organów administracji publicznej, jak i operatorów IK, społeczeństwa, gospodarki i państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji" [3]; współpracę oznaczającą „wykonywanie razem przez uczestników ochrony IK określonych, zbieżnych i wzajemnie uzupełniających się zadań dla osiągnięcia wspólnego celu, który wynika z zasady współodpowiedzialności. Współpraca jest niezbędna w przypadku chęci uniknięcia powielania działań i ponoszonych kosztów oraz efektywniejszego wykorzystania posiadanych sił i środków" [3]; zaufanie – trzeci filar systemu ochrony infrastruktury krytycznej – rozumiane jako „przekonanie, że motywacją działania uczestników ochrony IK (dotyczy to w szczególności administracji i operatorów IK) jest dążenie do wspólnego celu – poprawy bezpieczeństwa IK i RP. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa" [3].

Syntetyczne zestawienie szans i zagrożeń dla zarządzania bezpieczeństwem infrastruktury krytycznej, które wynikają z Narodowego Programu Ochrony Infrastruktury Krytycznej, zawarto w tabeli 1.

Narodowy Program Ochrony Infrastruktury Krytycznej wraz z załącznikami jest dokumentem, który zawiera podstawowe informacje na temat między innymi technicznych, organizacyjnych i zapobiegawczych aspektów ochrony infrastruktury krytycznej oraz służy jako zestaw konkretnych wskazówek dotyczących budowy i funkcjonowania systemu ochrony infrastruktury krytycznej, zapobiegając wybranym zagrożeniom. W tym kontekście można dostrzec potencjał do rozwoju systemów ochronnych, biorąc też pod uwagę miniaturyzację bezzałogowych statków powietrznych naszpikowanych elektroniką, które służą do zdobywania informacji, ale także do bezpośredniego ataku.

W tabeli 2 na podstawie dostępnych raportów (The Global Risk Report) za lata 2021 i 2022 odniesiono się do możliwych zagrożeń dla bezpieczeństwa infrastruktury krytycznej oraz określono poziom ich wpływu na zarządzanie bezpieczeństwem takich systemów.

Tab. 1. Szanse i zagrożenia dla zarządzania bezpieczeństwem infrastruktury krytycznej wynikające z Narodowego Programu Ochrony Infrastruktury Krytycznej

Szanse	Zagrożenia
– wypracowanie przejrzystych zasad i procedur między organami i służbami państwa a właścicielami oraz posiadaczami samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej; – uznanie ochrony IK jako procesu ukierunkowanego na ochronę ciągłości świadczenia określonej usługi oraz odtworzenia jej w razie potrzeby	– partnerstwo międzysektorowe oznacza jedynie ograniczoną formę współpracy między jednostkami administracji publicznej a podmiotami prywatnymi, poprzez na przykład wymianę wszelkich informacji mogących mieć wpływ na osiągnięcie celów NPOIK – takie partnerstwo nie przewiduje natomiast zawarcia jakiejkolwiek umowy, na podstawie której następowałaby realizacja za wynagrodzeniem przez partnera prywatnego przedsięwzięcia na rzecz podmiotu publicznego; – identyfikacja słabości procedury nakładania na operatorów infrastruktury krytycznej obowiązków w drodze ustaw czy rozporządzeń ze względu na realny brak możliwości prowadzenia audytu i kontroli ich realizacji

Źródło: opracowanie własne

Tab. 2. Szacowany poziom wpływu zagrożeń na zarządzanie bezpieczeństwem infrastruktury krytycznej

Zagrożenia	Niski	Średni	Wysoki
Ekstremalne zjawiska pogodowe		**X**	
Awaria systemu cyberbezpieczeństwa			**X**
Ataki terrorystyczne			**X**
Awaria infrastruktury IT			**X**
Atak bronią masowego rażenia		**X**	
Upadek państwa	**X**		
Niekorzystny rozwój technologiczny		**X**	
Migracja przymusowa	**X**		
Załamanie w stosunkach międzypaństwowych	**X**		
Katastrofy geofizyczne			**X**

Źródło: opracowanie własne na podstawie następujących raportów: WEF_The_Global_Risks_Report_2021.pdf [4], WEF_The_Global_Risks_Report_2022.pdf [5]

Creative Commons Attribution 4.0 International License (CC-BY)

Bezzałogowe statki powietrzne (BSP) zwane potocznie dronami (ang. UAV – *Unmaned Aerial Vehicle*) stanowią naturalną konsekwencję rozwoju technologicznego i mogą być wykorzystywane m.in. w celach badawczych, ratowniczych, pomiarowych lub diagnostycznych, wspierając człowieka w jego działaniach na rzecz poprawy bezpieczeństwa oraz jakości życia. Jednak, jak wszystkie zdobycze techniki, BSP mogą również być użytkowane w sposób, który będzie zagrażał zdrowiu i życiu człowieka, jego mieniu lub środowisku naturalnemu.

Drony stają się dostępne dla każdego, a ich cena w odniesieniu do parametrów lotu i masy jest coraz niższa. Powoduje to powszechne wykorzystanie dronów, a jednocześnie generowanie coraz większej liczby zagrożeń, które można generalnie podzielić na następujące kategorie [6]:

- w transporcie – w tym w ruchu lotniczym (kolizja UAV z pojazdem, statkiem powietrznym lub odwrócenie uwagi kierującego),
- terroryzm (bezpieczeństwo transportu i infrastruktury krytycznej, obszary gęsto zaludnione, imprezy masowe),
- przemyt (granice – ominięcie odprawy, obiekty ochrony specjalnej),
- zagrożenia dla mienia,
- szpiegostwo (naruszenie prywatności, szpiegostwo przemysłowe, podsłuch, szpiegostwo instytucji i osób publicznych, agencji rządowych, instalacji wojskowych),
- zagrożenia dla środowiska naturalnego (hałas, ogień, płoszenie dzikich zwierząt) [6].

Zagrożenia płynące ze strony BSP działającego autonomicznie i zaprogramowanego na lot po wyznaczonych punktach GPS są znacznie większe z uwagi na możliwość jego działania bez aparatury RC i braku możliwości detekcji tego typu łączności. Niezwykle duże zagrożenie w poruszaniu się pojazdami bezzałogowymi niesie ze sobą także współdzielenie przestrzeni lotu z innymi obiektami. Największe niebezpieczeństwo dla człowieka występuje tutaj w przypadku pojazdów lądowych i powietrznych. Znajomość prawa o ruchu drogowym jest znacznie powszechniejsza niż wiedza o zasadach korzystania ze wspólnej przestrzeni powietrznej według prawa lotniczego. Zderzenie pojazdu bezzałogowego z pojazdem przewożącym ludzi może spowodować uszkodzenie i awaryjne lądowanie. Przykładowo, bezzałogowe statki powietrzne wykorzystywane amatorsko do obserwacji pożaru wymusiły na śmigłowcach gaśniczych wyższy pułap lotu, uniemożliwiając dokładny zrzut wody [9].

Pojazdy bezzałogowe stanowią bardzo poważne zagrożenie szczególnie dla silników statków powietrznych i – pośrednio – dla ich obsługi. Już samo współużytkowanie przestrzeni powietrznej przy zachowaniu separacji wysokości jest wyzwaniem.

Bezzałogowy statek powietrzny w swej najprostszej definicji jest maszyną, która nie wymaga do lotu załogi obecnej na pokładzie, nie ma możliwości zabierania

pasażerów i jest pilotowany zdalnie lub wykonuje lot autonomicznie. W rzeczywistości sam statek powietrzny potrzebuje do działania dodatkowych zasobów i urządzeń. Urządzenia te wzajemnie się komunikują i umożliwiają statkowi wykonanie powierzonego mu zadania [11].

Sama nazwa dron wywodzi się od angielskiego *drone*, co oznacza trutnia. Dziedzina dronów – wielowirnikowce, które zdobyły największą popularność ostatnimi latami, podczas latania wydają charakterystyczny dźwięk, który wytwarzają szybko kręcące się śmigła, podobny do latających trutni. Bezzałogowe statki powietrzne możemy podzielić na kilka kategorii, w zależności od budowy i napędu: wielowirnikowce, płatowce, śmigłowce oraz hybrydy.

Bezzałogowy statek powietrzny jest wyposażany w różnego rodzaju efektory (sensory radiolokacyjne, głowice optoelektroniczne, analizatory widma, sensory akustyczne), które służą do: obserwacji, przekazania informacji oraz rażenia przeciwnika. Urządzenie to może też służyć jako zwykły transporter lotniczy do przenoszenia ładunków wybuchowych, broni, środków trujących czy przemytu narkotyków przez granice państwa. Samo urządzenie w zetknięciu z innym uczestnikiem ruchu, samolotem czy samochodem stanowi poważne zagrożenie dla lotnisk, autostrad czy innych składników infrastruktury krytycznej itp. Pomimo zakazu lotów zdarzają się przypadki notorycznego ich łamania. Dron to urządzenie latające, które porusza się z małą prędkością i na małych wysokościach, co utrudnia ich wykrycie. Dodatkowo posiadają one jeszcze bardzo małą skuteczną powierzchnię odbicia, wskutek czego są bardzo trudne do rozpoznania przez radar. Problemem staje się też ustalenie właściciela lub pilota statku. Sterowanie nim odbywa się bowiem z dużej odległości na przykład za pomocą sieci internetowej LTE. Może to odbywać się z laptopa z dowolnego miejsca na świecie. Wraz z rozwojem technologii zmieniane są przepisy prawa lotniczego, które dzisiaj zabrania sterowanie dronem bez posiadania uprawnień, chyba że jego waga nie przekracza 0,6 kg. Bezzałogowy statek powietrzny może być wykorzystany w pozytywnym znaczeniu jako pomiar geodezyjny czy wykonanie zdjęć z powietrza. Jednak istnieje niebezpieczeństwo, że może nastąpić przechwycenie sygnału sterującego i bezzałogowy statek powietrzny zmieni właściciela.

Dzisiejszy dron wykorzystany przeciwko infrastrukturze krytycznej stanowi dla niej wyzwanie. Drony są bardzo ciche, nie można ich usłyszeć i dostrzec, a są zdolne do szpiegostwa infrastruktury technicznej. Trzeba mieć świadomość, że przestrzeń powietrzna wokół infrastruktury krytycznej jest najsłabiej zabezpieczona i praktycznie można bezkarnie wykonywać loty przez wykorzystanie bezzałogowych statków powietrznych.

W literaturze przedmiotu wskazano, że najbardziej podatnymi na atak ze strony dronów są takie elementy infrastruktury krytycznej, jak: systemy zaopatrzenia w energię, surowce energetyczne i paliwa; systemy łączności; systemy sieci teleinformatycznych, systemy produkcji, składowania, przechowywania i stosowania

Creative Commons Attribution 4.0 International License (CC-BY)

substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. W tych przypadkach ryzyko jest nieakceptowalne. Systemy ratownicze także są obarczone dużym ryzykiem, jednak w mniejszym stopniu niż wyżej wskazane. Pozostałe systemy mieszczą się w grupie ryzyka „do zaakceptowania".

Współcześnie bezpieczeństwo infrastruktury krytycznej nie tylko stanowi podstawę działania państwa, ale wręcz jest warunkiem *sine qua non* jego funkcjonalnego istnienia. W związku z tym operatorzy i użytkownicy samoistni systemów IK podejmują działania, których zadaniem jest jak najskuteczniejsza ochrona usług, bez których trudno sobie wyobrazić nowoczesne państwo. Jednym z kluczowych elementów tych działań jest niewątpliwie stworzenie odpowiedniego otoczenia regulacyjnego. Prawodawstwo w zakresie infrastruktury krytycznej musi zmierzyć się z trzema głównymi wyzwaniami [13]: przewidzeniem rodzaju i intensywności potencjalnego kryzysu mogącego negatywnie wpłynąć na infrastrukturę krytyczną; zapewnieniem odpowiednich narzędzi reakcji na kryzys; zachowaniem proporcjonalności stworzonych narzędzi, poprzez maksymalizację ochrony bezpieczeństwa publicznego i minimalizację negatywnego wpływu na wolności jednostek.

Pozyskanie pełnej wiedzy o wszystkich zagrożeniach jest praktycznie niemożliwe. Głównie dlatego, że różnorodność zjawisk stanowiących zagrożenie osiągnięcia zamierzonych celów przez przedsiębiorstwo jest ogromna. Niebezpieczeństwa te rodzą się w różnych uwarunkowaniach organizacyjno-prawnych, ekonomiczno-finansowych, techniczno-technologicznych i innych. Oznacza to powstawanie nowych rodzajów ryzyka i metamorfozę już istniejących.

Logiczną reakcją organizacji na zakłócenia jest budowanie mechanizmu samoregulacji opartej na monitorowaniu zagrożeń, neutralizowaniu ich, a gdy to się nie uda, na przywracaniu stanu sprzed zakłócenia, zaś do tego czasu zapewnianiu form działania zastępczego. Postępowanie takie jest wyrazem racjonalnego reagowania na nieuniknione ryzyko. Szczegółowe analizowanie mechanizmu takiego postępowania prowadzi do określenia kryteriów racjonalnego oceniania ryzyka oraz modelowych postaw reagowania, stosownych do rozmiarów potencjalnego oddziaływania ryzyka. W szczególności racjonalność reagowania opiera się na ocenie czynników intensywności ryzyka, tj. siły jego wpływu (zwłaszcza potencjalnych szkód) oraz częstości oddziaływania [13].

Ciągłość działania, po pierwsze, jest postulatem doskonałości systemu działania, jakim jest każda organizacja, a więc i każdy podmiot gospodarczy czy administracyjny. W tym sensie zapewnianie ciągłości działania jest przedmiotem zarządzania strategicznego, wyrażając cel nadrzędny sprawności organizacji i obejmując prymat w obszarze zarządzania ryzykiem operacyjnym.

Po drugie, ciągłość działania jest rozumiana jako postępowanie organizatorskie tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia będącego wynikiem swoistej interakcji przejawów zagrożenia z podatnością organizacji wewnętrznej, infrastruktury lub zasobów. W tym sensie

zapewnianie ciągłości działania jest przedmiotem zarządzania operacyjnego i stanowi ostatnie ogniwo zarządzania ryzykiem operacyjnym.

Uogólniając, ciągłość działania to zdolność organizacji do takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, szybko przywrócić te normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań. Ciągłość działania postrzega się więc w kontekście zadań organizacji oraz procesów służących realizacji tych zadań, jak i w kontekście czynników mogących zakłócić te procesy oraz form podatności organizacji stanowiących o jej wrażliwości na zakłócenia.

Zapewnianie ciągłości działania obejmuje [13]:

- mechanizm reagowania organizacji na zakłócenia,
- proces rozwijania ww. mechanizmu zdolności reagowania na zakłócenia (jako proces – w rozumieniu analizy procesowej – podstawową działalność organizacji),
- proces zarządzania bieżącą zdolnością zapewniania ciągłości działania oraz jej stałym doskonaleniem.

Na mechanizm reagowania na zakłócenia składają się [13]: struktura organizacyjna dedykowana do zadania zapewniania ciągłości, stanowiąca spójną całość z ogólną strukturą organizacyjną; formalne uregulowania organizacyjne określające relacje w strukturze organizacyjnej związane z zadaniem zapewniania ciągłości; utrwalona praktyka (możliwie spisana) postępowania w sytuacjach, gdy wymagana jest reakcja na zaistniałe zakłócenie.

Przede wszystkim należy podkreślić, że reagowanie na zakłócenia poprzez zapewnianie ciągłości działania należy rozumieć nie tylko jako bezpośrednie postępowanie wobec zakłóceń, ale także jako aktywność o charakterze prewencyjnym, związaną z analizą zagrożeń i podatności oraz z poszukiwaniem metod i rozwiązań zapobiegania zaistnieniu zakłóceń. W tym sensie starania o ciągłość działania i bezpieczeństwo splatają się. Z punktu widzenia ciągłości działania rozwiązania bezpieczeństwa zapewniają prewencję wobec zagrożeń, zaś z punktu widzenia bezpieczeństwa rozwiązania ciągłości działania stanowią dodatkowe zabezpieczenie. Uzasadnia to koncepcję wspólnego zarządzania obydwoma zagadnieniami, a podobnie i zarządzaniem jakością [13].

Zagrożenie bezzałogowymi statkami powietrznymi dla infrastruktury krytycznej jest realne. Drony poprzez możliwości różnorodnego wykorzystania sprawiają, że pojawiają się nowsze i bardziej dopracowane konstrukcje. W rezultacie może to stanowić problem nawet dla najnowocześniejszych systemów antydronowych.

Potencjalni terroryści, którzy dopuszczają się ataku na obiekty IK, najprawdopodobniej posłużą się dronami bardzo lekkimi lub lekkimi. Są one dostępne niemal wszędzie i bez większych problemów. Nie sprawiają także kłopotów z obsługą, a ich cena jest na tyle niska, że nawet ich zniszczenie przy niepowodzeniu potencjalnego aktu terroru nie jest bardzo odczuwalne. Drony lekkie nie przeniosą

Creative Commons Attribution 4.0 International License (CC-BY)

wprawdzie ciężkich ładunków, ale już niewielka ilość bakterii wąglika jest w stanie zabić wiele osób. Można również doczepić do drona kamerę cyfrową, która pozwoli potencjalnym terrorystom na zapoznanie się z topografią terenu danego obiektu IK, który jest ich celem.

Bezzałogowych statków powietrznych wyposażonych w dobrą optykę z rejestracją obrazu (na wewnętrznym dysku lub z możliwością bezpośredniego przesyłu obrazu do operatora) potencjalni terroryści mogą używać do sporządzenia mapy lokalizacyjnej punktu, na który atak będzie najbardziej odczuwalny i powodujący najwięcej zniszczeń. Takie skutki miałby atak na obiekt z sektora przemysłu paliwowego i energetycznego. Przykładowo podczas ataku terrorystycznego z użyciem drona na sektor energetyczny może dojść do tzw. blackoutu, czyli braku napięcia w sieci elektroenergetycznej na znacznym obszarze [14].

Obecnie poszukuje się zaawansowanych form ochrony, które stanowią główne lub uzupełniające narzędzie do zapewnienia bezpieczeństwa, prewencji, ochrony i zarządzania. Dąży się do osiągnięcia stanu braku zagrożenia, dającego pewność i gwarancję utrzymania poczucia bezpieczeństwa. Potrzeba braku zagrożenia dała impuls do wdrażania inteligentnych systemów zabezpieczeń do monitorowania, nadzorowania, sygnalizacji i patrolowania. Drony na rzecz bezpieczeństwa publicznego z powodzeniem mogą być wykorzystywane np. do monitorowania i kontroli miejsc trudno dostępnych lub niebezpiecznych; monitorowania stanu technicznego obiektu w kontekście wczesnej identyfikacji zagrożenia; weryfikacji alarmu; patrolowania z powietrza; kontroli stanu ilościowego towaru w przypadku podejrzenia kradzieży.

Z drugiej strony można spotkać się z nieuprawnionymi próbami użycia BSP w kontekście naruszenia prywatności, działań przemytniczych, szpiegowskich czy terrorystycznych na obiekty publiczne czy infrastruktury krytycznej. Każde takie nieuprawnione działanie ma za zadanie pozyskanie informacji o danym celu, rozpoznanie obiektu w celach rabunkowych, pozyskanie wiedzy o modelu prowadzonej działalności czy zbieranie danych o rozwoju firmy, co dotyczy zwłaszcza zakładów produkcyjnych. Lista obiektów zagrożonych niepożądanymi działaniami dronów się wydłuża. Wynika to z coraz większej świadomości po stronie zarządzających danymi miejscami. Przedsiębiorcy dużych zakładów produkcyjnych, firm logistyczno-spedycyjnych, obiektów infrastruktury krytycznej, rządowych, rekreacyjno-sportowych i prywatnych dostrzegają problem szeroko pojętej inwigilacji przez dokonujących nieuprawnione loty nad ich obiektami. Powyższe działania stanowią podstawę dla producentów do tworzenia coraz nowocześniejszych urządzeń czy systemów do identyfikacji i neutralizacji dronów w sytuacji zagrożenia.

4. Podsumowanie

Podsumowując, można wskazać na szereg rekomendacji, które powinny zostać rozważone podczas użytkowania systemów infrastruktury krytycznej państwa. Rekomendacje sprowadzają się do postulatu głównego, że niezbędne jest bardzo szerokie wprowadzenie skutecznych systemów ochronnych, w tym antydronowych. Tego typu systemy są już opracowane lub są w końcowych stadiach certyfikacji. Systemy są różnorodne i można je dowolnie konfigurować w zależności od potrzeb i posiadanych środków finansowych na ochronę IK. Wprowadzenie skutecznych systemów antydronowych pozwoli na skuteczne zarządzanie bezpieczeństwem infrastruktury krytycznej państwa. Ponadto wskazać można na ogólne rekomendacje.

1. Najbardziej podatnymi na zagrożenia o dużym potencjale wystąpienia zagrożenia ze strony dronów są takie elementy infrastruktury krytycznej, jak: systemy zaopatrzenia w energię, surowce energetyczne i paliwa; systemy łączności; systemy sieci teleinformatycznych, systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych oraz systemy ratownicze. Logiczną reakcją organizacji na zakłócenia jest budowanie mechanizmu samoregulacji opartej na monitorowaniu zagrożeń, neutralizowaniu ich, a gdy to się nie uda, na przywracaniu stanu sprzed zakłócenia, zaś do tego czasu zapewnianiu form działania zastępczego. Postępowanie takie jest wyrazem racjonalnego reagowania na ryzyko.
2. Wszystkie wyżej wskazane elementy mają wpływ na zarządzanie bezpieczeństwem, które w wielkim stopniu opiera się na zapewnieniu ciągłości działania. W tym sensie zapewnianie ciągłości działania jest przedmiotem zarządzania strategicznego, wyrażając cel nadrzędny sprawności organizacji i obejmując prymat w obszarze zarządzania ryzykiem operacyjnym.
3. Niezwykle istotna dla systemów IK jest ciągłość działania rozumiana jako postępowanie organizatorskie, tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia będącego wynikiem swoistej interakcji przejawów zagrożenia z podatnością organizacji wewnętrznej, infrastruktury lub zasobów. W tym sensie zapewnianie ciągłości działania jest przedmiotem zarządzania operacyjnego i stanowi ostatnie ogniwo zarządzania ryzykiem operacyjnym.
4. Niezwykle ważnym wnioskiem wydaje być taki oto, że takie same zagrożenia ze strony UAV, jakie zostały zidentyfikowane, mogą być ukierunkowane na inne systemy w państwie. Przede wszystkim można tu myśleć o systemach związanych z obronnością, sferą bezpieczeństwa państwa.

Creative Commons Attribution 4.0 International License (CC-BY)

Bibliografia/References

1. Ustawa z 27 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2022 r. poz. 261, 583).
2. https://www.gov.pl/web/rcb.
3. Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022" (M.P. z 16 maja 2013 r. poz. 377).
4. WEF_The_Global_Risks_Report_2021.pdf.
5. WEF_The_Global_Risks_Report_2022.pdf.
6. Fellner R., Mańka A., *Kursy operatorów bezzałogowych statków powietrznych – „Prawo jazdy na drony (UAV)"*, www.bsp.2ap.pl, www.ktl.polsl.pl.
7. Tuśnio N., Nowak A., Tuśnio J., Wolny P., *Bezzałogowe statki powietrzne w działaniach Państwowej Straży Pożarnej – propozycja dedykowana Państwowej Straży Pożarnej*, „Zeszyty Naukowe SGSP" 2016, 58, tom 1/2.
8. Polkowski P., *Bezzałogowe statki powietrzne unmanned aerial vehicles*, „Rocznik Bezpieczeństwa Międzynarodowego" 2016, 10(1).
9. Holliday B., *Drones: The Complete Collection*, CreateSpace Independent Publishing Platform, 2017.
10. Zawiła-Niedźwiecki J., *Ciągłość działania organizacji*, „Prace Naukowe Politechniki Warszawskiej. Organizacja i Zarządzanie Przemysłem" 2008, z. 20, 3–7.