ZABEZPIECZENIE PORTÓW MORSKICH I OCHRONA INFRASTRUKTURY KRYTYCZNEJ
PROTECTION OF SEA HARBOURS AND CRITICAL INFRASTRUCTURE PROTECTION

Iwona DUDZIUK
iwonadudziuk7@gmail.com

Akademia Marynarki Wojennej
Wydział Dowodzenia i Operacji Morskich
Instytut Bezpieczeństwa Publicznego

Ewa IWANINA-SZOPIŃSKA
iwaninaszopinska@gmail.com

Akademia Marynarki Wojennej
Wydział Dowodzenia i Operacji Morskich
Instytut Operacji Morskich

STRESZCZENIE

Porty morskie, jako punkty węzłowe na styku lądu z morzem są znaczącym ogniwem w systemie gospodarczym państwa. Ważne jest, aby ich bezpieczeństwo było utrzymywane na najwyższym możliwym poziomie. W związku z tym dzięki współczesnemu rozwojowi techniki i technologii możemy wykorzystywać systemy bezzałogowych statków - dronów do ich ochrony i obrony, szczególnie skupiając się na obiektach infrastruktury krytycznej. Mogą one pracować w środowisku lądowym oraz morskim. Dostosowując parametry i zadania do potrzeb, możemy nie tylko monitorować określone obszary, ale również niszczyć niepożądane obiekty, aby zapewnić maksimum bezpieczeństwa w portach.

SUMMARY

Sea harbours as key nodal points based at the land-sea interface are a significant link in the state's economic system. It is extremely important to keep their safety at the highest level. Therefore, due to the development of technology we can use unmanned ships – drones for their protection and defence especially focusing on the critical infrastructure facilities. They are able to work on land as well as on the sea. Furthermore, they easily adjust their parameters and tasks to meet all the needs. Finally we are able to monitor specific areas as well as destroy undesirable objects to provide maximum safety in the harbours.

Słowa kluczowe: bezzałogowe statki, ochrona portu, infrastruktura krytyczna, bezpieczeństwo
Key words: unmanned ship, harbour protection, critical infrastructure, safety

WSTĘP

Problem skutecznej ochrony infrastruktury krytycznej znalazł swoje odzwierciedlenie w obowiązującym ustawodawstwie. Jej ochrona stała się priorytetem dla organizacji bezpieczeństwa państwa. Stworzono szereg kryteriów, według których obiekty, urządzenia

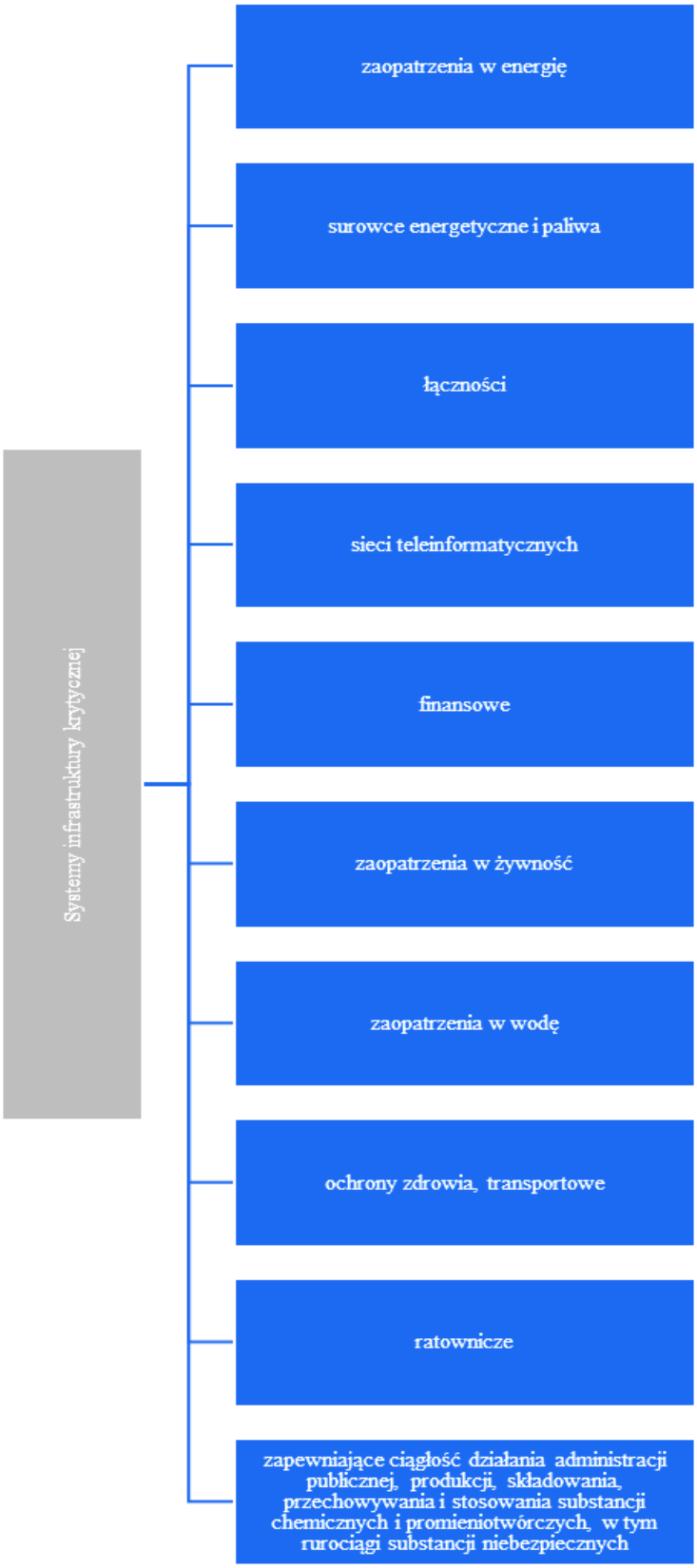
i systemy są klasyfikowane. Jednak niejednoznaczny podział kompetencji organów odpowiedzialnych za wytypowanie obiektów o krytycznym znaczeniu dla państwa oraz określenie strategicznych celów ich ochrony może przyczynić się do wystąpienia zagrożeń. Nie należy zapominać, że część tej infrastruktury znajduje się w rękach prywatnych, w związku z tym wymaga to odpowiedniej współpracy między gestorami poszczególnych systemów i świadomości, że w przypadku wystąpienia zakłóceń i nieprawidłowości skutki mogą objąć nie tylko bezpośrednich użytkowników infrastruktury, ale też mieć charakter państwowy (Milewski, 2016). Współczesne tempo rozwoju techniki i technologii powoduje znaczne poszerzenie obszaru możliwych do wystąpienia zagrożeń oraz ich modyfikacji. Coraz więcej obiektów, systemów i urządzeń o istotnym znaczeniu dla gospodarki i państwa, funkcjonuje obecnie w tzw. obszarach połączonych, które ze względu na swoją różnorodną użyteczność gospodarczą lub przemysłową stanowią względną całość jako połączony ze sobą system tak jak porty morskie. Tym samym ochrona jednego z jej elementów stanowi o ochronie całości.

1. DOBÓR OBIEKTÓW DO INFRASTRUKTURY KRYTYCZNEJ

Infrastruktura krytyczna (IK) to, według ustawy o zarządzaniu kryzysowym, wszystkie systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty: budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli, które mają służyć zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców (Ustawa o zarządzaniu kryzysowym, 2007). To rzeczywiste i cybernetyczne systemy niezbędne do minimalnego funkcjonowania gospodarki i państwa. Nie każdy strategiczny obiekt należy do niej. O tym co zaliczymy do IK decydują szczegółowe kryteria a lista takich obiektów znajduje się w załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), jednak ich treść jest niejawna ze względu na swój charakter (Rcb.gov.pl, 2018). Obejmują one szereg systemów przedstawionych na poniższym schemacie (Rysunek 1.).

Ważne jest, aby odpowiednio zabezpieczyć obiekty infrastruktury krytycznej. Jej ochrona polega na zorganizowaniu szeregu przedsięwzięć realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. Zagrożeniami dla infrastruktury krytycznej są zagrożenia naturalne - spowodowane czynnikami niezależnymi od człowieka, zdarzenia wywołane działaniem człowieka w tym zagrożenia militarne (atak

zbrojny, dywersja militarna), niemilitarne (ekonomiczne, społeczne, ekologiczne) oraz terrorystyczne (w tym militarne działania nieregularne).



Rys. 1. Systemy infrastruktury krytycznej
Źródło: Opracowanie własne na podstawie (Rcb.gov.pl, 2018).

Mówiąc o *systemie* mamy na myśli zespół wzajemnie powiązanych ze sobą, sprzężonych elementów, spełniających określoną funkcję i traktowanych jako wyodrębniony element z otoczenia w określonym celu (Encyklopedia.pwn.pl, 2018). Tym celem jest bardzo często sposób przeznaczenia i wykorzystania pojedynczego elementu lub jego całości. Infrastruktura krytyczna obejmuje systemy zaopatrzenia m.in. w energię, paliwa i surowce energetyczne. Ochrona przed czynnikami zagrażającymi ciągłości zaopatrzenia w powyższe surowce wpływa negatywnie i osłabiająco na pozostałe jego istniejące elementy, np. na system transportowy czy też łączności i sieci teleinformatycznych.

Aby obiekt, urządzenie, instalacja lub usługa mogły być zakwalifikowane jako infrastruktura krytyczna musi ona spełnić szereg kryteriów.

Kryteria wyboru infrastruktury krytycznej są podzielone są na dwie grupy:

1) kryteria sektorowe (systemowe), charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do elementów infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK;

2) kryteria przekrojowe, opisujące parametry odnoszące się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi (Szewczyk, Pyznar, 2018).

Zgodnie z przyjętą metodyką wszystkie trzy niżej przedstawione kroki muszą być zrealizowane aby mówić o infrastrukturze krytycznej:

1) w kroku pierwszym – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria sektorowe (systemowe), właściwe dla danego systemu IK;

2) w kroku drugim – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w drodze spełnienia pierwszego kroku należy zastosować definicję zawartą w art. 3 pkt. 2 ustawy o zarządzaniu kryzysowym;

3) w kroku trzecim – w celu wskazania, jakie będą skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w drodze spełnienia kroku pierwszego i drugiego należy zastosować kryteria przekrojowe (należy wybrać kryteria najlepiej odzwierciedlające charakterystykę systemu), przy czym aby wypełnić krok trzeci,

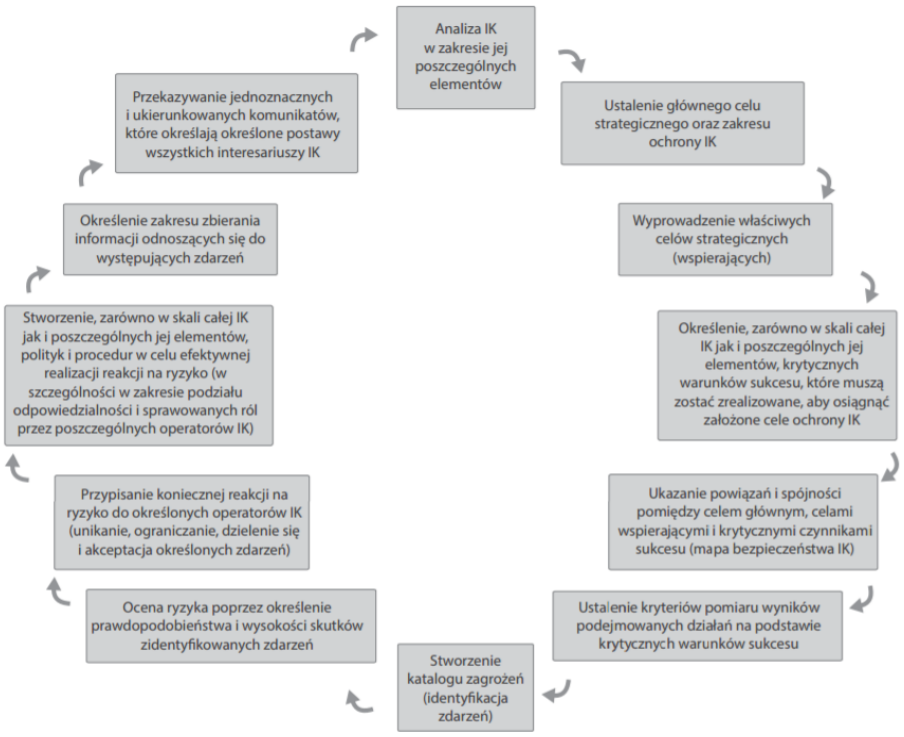
potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe (Szewczyk, Pyznar, 2018).

Wyżej wymienione systemy, które możemy rozpatrywać pojedynczo, a także łącząc je z poszczególnymi innymi systemami, które stają się bardziej złożone, stanowią wrażliwy punkt. Tym samym zyskują status obszarów szczególnych. W dobie wzajemnych powiązań dotyczących procesu zapewnienia bezpieczeństwa, a także troski o pewien obszar funkcjonowania należy obejmować działaniami zabezpieczającymi całość elementów tworzących określony system a nie tylko jego pojedyncze komórki. Z uwagi na często subiektywne rozumienie pojęcia infrastruktura krytyczna a skali skutków, które mogą powstać, świadomość jej ochrony musi być coraz większa, nie tylko w skali całego kraju, województwa czy powiatu, ale też lokalnie np. w określonych przedsiębiorstwach, w których takie obiekty, instalacje czy systemy występują.

2. POPRAWA BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ

Infrastruktura krytyczna spełnia kluczową rolę w funkcjonowaniu poszczególnych ośrodków (regiony, w których infrastruktura krytyczna stanowi podstawowe źródło pracy i finansowania), co przekłada się w jawny sposób na funkcjonowanie państwa i jego społeczeństwa. Dbałość o nieprzerwane funkcjonowanie systemów IK stanowi, a co najmniej powinno stanowić, priorytet ciągłego tworzenia nowych procedur, udoskonalania ich czy podnoszenia jakości działań. Każde zdarzenie, które powoduje jakiekolwiek zakłócenia czy przerwanie funkcjonowania infrastruktury krytycznej, powinno powodować podjęcie szeregu działań w celu jego identyfikacji oraz próbę wyeliminowania. Zadanie to stoi przed zarządcami, którzy bezpośrednio odpowiadają za poszczególne obiekty, instalacje i systemy ale również przed całą administracją publiczną. Ustawa o *Zarządzaniu kryzysowym* określa właściwe organy odpowiedzialne za sprawy zarządzania kryzysowego. Ponadto określa zadania stawiane przed nimi w celu zapobiegania oraz przygotowania na nie za pomocą sprawdzonych działań i określonych procedur. Reagowanie na zdarzenia kryzysowe jest tak naprawdę testem określającym odpowiedni: poziomu przygotowania, stopień zabezpieczenia ilościowego i jakościowego sprzętu oraz scenariusz procedur podejmowania skutecznych reakcji. Po wystąpieniu zagrożenia i przejęcie kontroli nad nimi dalsze działania sprowadza się do odtwarzania do istniejącego wcześniej stanu lub całkowitej jego odbudowy. Ochrona infrastruktury krytycznej to zespół przedsięwzięć organizacyjnych podejmowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia obiektów, przywrócenia

funkcjonalności systemów, sieci itd. (Rysunek 2.) (Ustawa o zarządzaniu kryzysowym, 2007). Zwrócenie uwagi na ważność prawidłowego działania infrastruktury krytycznej przyczyniło się do powstania już wcześniej wspomnianego Narodowego Programu Ochrony Infrastruktury Krytycznej.



Rys. 2. Proces zapewniania bezpieczeństwa infrastruktury krytycznej
Źródło: Pyznar i in. 2014.

Podstawowym celem stworzenia programu NPOIK była poprawa bezpieczeństwa w zakresie IK na terenie przedsiębiorstwa, gminy, powiatu, województwa oraz całego państwa.

Osiągnięcie tego celu wymaga realizacji szeregu zadań pośrednich:

- podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa oraz sposobów jej ochrony, Narodowy Program Ochrony Infrastruktury Krytycznej;
- określenie ról i zakresu odpowiedzialności podmiotów publicznych i prywatnych uczestniczących w działaniach na rzecz ochrony IK;
- 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;
- przygotowanie strategicznego programu podniesienia bezpieczeństwa IK oraz wsparcia wybranych programów badawczych i rozwojowych, edukacyjnych i szkoleniowych ukierunkowanych na podnoszenie odporności infrastruktury (Rcb.gov.pl, 2018).

Podstawowymi i najważniejszymi zasadami NPOIK są (Rysunek 3.):

- *współodpowiedzialność* – wiodąca zasada przyjęta przy budowie systemu ochrony IK. Rozumiana jest 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 w konsekwencji państwa. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno jej operatorów, jak i odpowiedzialnej za funkcjonowanie państwa administracji;
- *współpraca* – drugi filar systemu ochrony IK. W kontekście programu oznacza 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. We wzajemnej współpracy administracji publicznej i sektora prywatnego tkwi potencjał, który z powodzeniem można wykorzystać. Warunkiem skutecznej współpracy są jej autentyczność, wzajemność i dążenie do wspólnej korzyści;
- *zaufanie* – trzeci filar systemu ochrony IK. W Programie 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. Osiągnięcie tego celu będzie zatem korzystne dla wszystkich zainteresowanych stron, w tym przede wszystkim społeczeństwa (Rcb.gov.pl, 2018).

Rys. 3. Zasady Narodowego Programu Ochrony Infrastruktury Krytycznej
Źródło: Opracowanie własne na podstawie Rcb.gov.pl (2018).

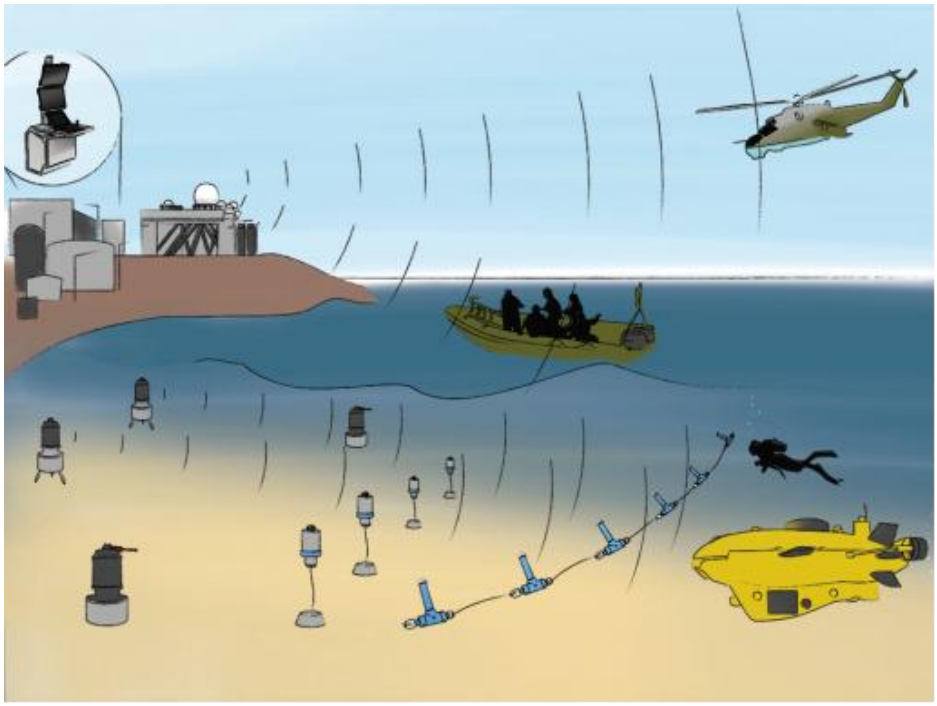
Jednym z narzędzi pozwalających kontrolować zagrożenia jest dobrze funkcjonująca infrastruktura krytyczna. Zwrócenie uwagi na wrażliwe elementy otoczenia człowieka oraz wskazanie ich charakterystycznych cech, a w konsekwencji stworzenie dedykowanych im szczególnych rozwiązań pozwoliło na ograniczenie ryzyka zaistnienia sytuacji dysfunkcji dostarczanych przez nie usług (Pyznar, i inni, 2014). Pojawia się jednak cały czas pytanie, jak zapewnić właściwą i skuteczną ochronę infrastruktury krytycznej?

3. MORSKA INFRASTRUKTURA KRYTYCZNA I JEJ OCHRONA

W rozumieniu ustawy z dnia 4 września 2008 r *o ochronie żeglugi i portów morskich* porty morskie to akweny i grunty oraz związana z nimi infrastruktura portowa, na obszarze których znajduje się jeden lub więcej obiektów portowych. Infrastruktura krytyczna w odniesieniu do obszarów morskich, szczególnie portów związana jest z zabezpieczeniem jej funkcjonalności zarówno od strony lądu, jak i wody. Procedury zabezpieczeń w tym przypadku nigdy nie będą takie same, ze względu na różne środowisko występowania, jednak działania powinny zostać ukierunkowane do jak największego ujednolicania oraz ich uniwersalności.

Dotychczasowe metody monitoringu i ochrony portów morskich w dobie rozwoju techniki i technologii stały się niewystarczające. Nowe zagrożenia wymuszają na zarządach portów, aby poszukiwały nowych rozwiązań w celu zapewnienia maksimum bezpieczeństwa. Dlatego bezzałogowe statki powietrzne, nawodne i podwodne, które wykorzystywane były głównie w obszarach działań militarnych czy celach rekreacyjnych przeniesiono na potrzeby przedsiębiorstw i ich ochrony. Dostrzeżono nowy potencjał i możliwości zastosowania bezzałogowych robotów m.in. do ochrony i obrony poszczególnych stref portowych. Obecny rynek bezzałogowców oferuje cały wachlarz dronów dedykowanych różnym środowiskom i zadaniom stawianym dla nich. Zakup i użytkowanie jest uzależnione m.in. od zasobów

finansowych, przeznaczenia, czasu i warunków pracy, a także odporności na zmienne warunki otoczenia i warunki meteorologiczne (ląd, woda, silny wiatr, inne obiekty, opady atmosferyczne). Urząd Morski w Słupsku pokazuje, iż takie działania przynoszą pozytywne korzyści. Bezzałogowy statek latający został zakupiony i wykorzystany do różnego rodzaju działań. Są to m.in.: poszukiwanie i ratownictwo dla potrzeb Morskiej Służby Poszukiwań i Ratownictwa (zarejestrowane filmy służą podczas realnych akacji a także podczas ćwiczeń), monitoring strefy brzegu morskiego, nadzór nad postępem wykonywania prac inwestycyjnych, ocena szkód posztormowych oraz wykorzystanie drona dla potrzeb geodezyjnych w celu zbierania dokładnych danych przestrzennych. Dzięki zastosowaniu tego typu urządzeń możliwe jest szybkie i skuteczne prowadzenie działań oraz dotarcie do miejsc, w których człowiek nie mógłby lub nie miał możliwości przebywać. Bezpośredni obraz i stan faktyczny monitorowanej sytuacji czy obiektu stanowi ogromną pomoc w reagowaniu na pojawiające się zagrożenia.



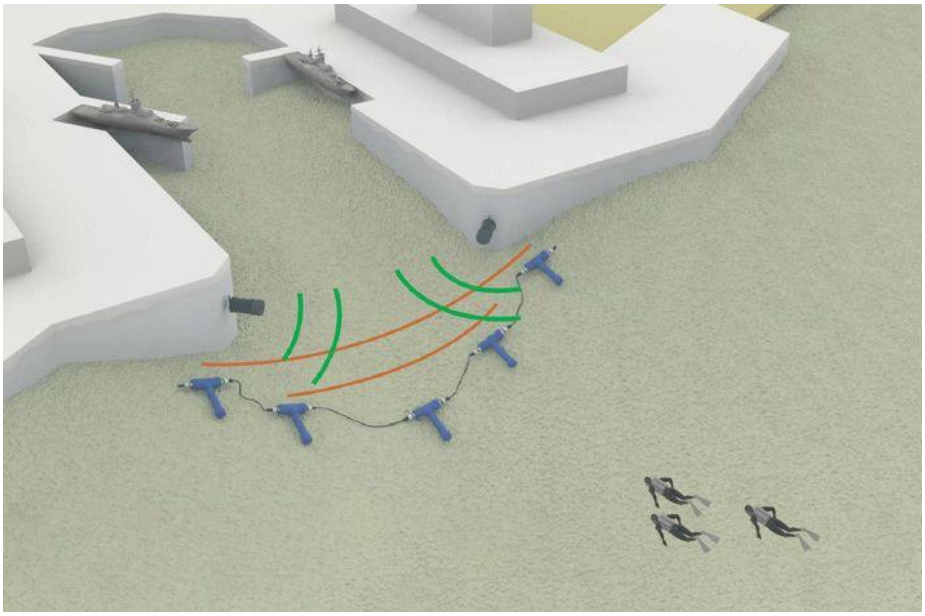
Rys. 4. System ochrony Morskiej Infrastruktury Krytycznej
Źródło:http://www.ctm.gdynia.pl/products/systemy-ochrony-infrastruktury-morskiej,12/system-ochrony-krytycznej-infrastruktury-morskiej,3.html (19.11.2017).

Innym sposobem ochrony potów jest zastosowanie nowoczesnych systemów ochrony morskiej infrastruktury krytycznej poprzez zastosowanie sensorów monitorujących sytuacje nawodną i podwodną w rejonach rozmieszczenia. Sensory te przeznaczone są do monitoringu i przeciwdziałania zagrożeniom dywersji podwodnej. Wykorzystują one konfigurację sensorów, które dodatkowo uzupełniane są przez zewnętrzne źródła informacji. Rozwiązanie

to oparte jest na połączeniu barier: pasywnej - magnetycznej oraz aktywnej - akustycznej, wyposażonych dodatkowo w czujniki takie jak: kamery, kamery na podczerwień, radary, pasywne anteny akustyczne, sonary i inne. Bariery magnetyczne reagują na środowiskowe zmiany pola magnetycznego wywołane ruchem obiektów generujących nawet słabe pole magnetyczne. Przekroczenia linii ochrony, utworzonej przez bariery: magnetyczną i hydroakustyczną, są wizualizowane pozycją na mapie chronionego obszaru, natomiast sonar DDS, czujniki w postaci kamery światła widzialnego oraz termowizyjnej rejestrującej promieniowanie podczerwone zapewniają obserwację obiektu oraz jego nawodne i podwodne śledzenie (Rysunek 4 oraz 5). Powyższy proces jest realizowany przez jednoczesną rejestrację i współbieżną analizę sygnałów z sensorów odbierających anomalie różnych pól fizycznych potencjalnych obiektów w podwodnej i nawodnej strefie chronionej zapewniając odpowiedni poziom prawdopodobieństwa wykrycia. Unikalność systemu jest wynikiem zastosowania zaawansowanych technologicznie sensorów: sonaru DDS do wykrywania nurków, monostatycznej bariery akustycznej oraz unikalnej technologicznie - bariery magnetycznej. Łańcuch sensorów magnetycznych wykrywa dowolny obiekt zwierający materiał ferromagnetyczny. Specjalna konstrukcja łańcucha umożliwia jego zainstalowanie na dnie lub zatopienie w błotnistym podłożu. Dodatkowo system ten posiada minimalne wymagania dotyczące utrzymania (Ctm.gdynia.pl,2017).

Korzyściami wynikającymi z posiadania takiego systemu są:

- zapewnienie bezpieczeństwa statków i sił morskich w porcie i na kotwicowiskach;
- monitoring nawodny i podwodny brzegu morskiego;
- monitoring infrastruktury portowej i kotwicowisk;
- odstraszanie nurków - dywersantów;
- podniesienie poziomu konkurencyjności portu i przyległej do niego infrastruktury;
- stworzenie bezpiecznych i atrakcyjnych ekonomicznie możliwości korzystania z portu (Ctm.gdynia.pl, 2017).



Rys. 5. Zabezpieczenie wejścia do portu Marynarki Wojennej
Źródło: https://www.defence24.pl/ctm-stworzylo-system-morskiej-ochrony-antyterrorystycznej (09.09.2018).

Powyższe systemy są doskonałym środkiem wspomagającym ochronę portów morskich. Musimy jednak pamiętać, iż nie są to najtańsze rozwiązania ekonomiczne. Dlatego ważne jest podjęcie wspólnych działań przez sektor publiczny i prywatny w celu zwiększenia bezpieczeństwa i zmniejszenia ryzyka wystąpienia potencjalnych zagrożeń. Warto również podkreślić, że jakikolwiek sprzęt, nawet najnowocześniejszy nie wykluczy czynnika ludzkiego, który jest obecny we wszystkich działaniach zmierzających do ochrony wszelakiej infrastruktury krytycznej. Na problemy bezpieczeństwa portu należy patrzeć nie tylko w świetle zdarzeń występujących na jego obszarze, ale również z perspektywy powiązań portów z ich dalszym zapleczem i przedpolem oraz ich miejscem w łańcuchu dostaw (Tubielewicz, Forkiewicz, 2018).

4. PODSUMOWANIE

Kluczowe dla bezpieczeństwa państwa i obywateli obiekty, instalacje, urządzenia i usługi Infrastruktury Krytycznej są niejawne i nie mogą być publicznie prezentowane. Ich lista (w związku z nowelizacją ustawy) uległa znaczącemu zwiększeniu. Dlatego zasadnym jest stworzenie warunków do poprawy jej bezpieczeństwa, co ma przyczynić się do podniesienia bezpieczeństwa Rzeczypospolitej Polskiej. Programy ochrony są adresowane przede wszystkim do administracji rządowej i jej operatorów, mogą być jednak stosowane przez wszystkich, którzy uznają je za pomocne w procesie zwiększania odporności na zakłócenia własnej infrastruktury, w tym samorządy i podmioty prywatne (Rcb.gov.pl, 2018). Porty morskie są ważnym, strategicznym elementem zarządzania kryzysowego łańcucha

dostaw, jak i elementem jego infrastruktury krytycznej. Prowadzi to do rozpatrywania infrastruktury portów morskich jako infrastruktury krytycznej kraju, a więc systemu powiązanych ze sobą obiektów (w tym budowli, urządzeń, instalacji, środków transportu bliskiego, usług) mających kluczowe znaczenie dla bezpieczeństwa państwa. Z tego powodu wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury portowej należy podejmować zgodnie z wymogami zarządzania kryzysowego i ochrony infrastruktury krytycznej systemu transportowego łańcucha dostaw. A wszelkie środki w tym nowoczesne systemy w postaci bezzałogowych statków czy technologie wykorzystujące sensory przyczyniają się do zwiększenia jego bezpieczeństwa (Tubielewicz, Forkiewicz , 2018).

LITERATURA

Ctm.gdynia.pl, (2017). *System Ochrony Krytycznej Infrastruktury Morskiej*, http://www.ctm.gdynia.pl/products/systemy-ochrony-infrastruktury-morskiej,12/system-ochrony-krytycznej-infrastruktury-morskiej,3.html (15.11.2017).

Defence24.pl, (2018). *Zabezpieczenie wejścia do portu Marynarki Wojennej* https://www.defence24.pl/ctm-stworzylo-system-morskiej-ochrony-antyterrorystycznej (09.09.2018).

Encyklopedia.pwn.pl, (2018). *System*. https://encyklopedia.pwn.pl/system.html (15.09.2017).

Milewski, J. (2016). *Identyfikacja infrastruktury krytycznej i jej zagrożeń.* Zeszyty Naukowe AON nr 4 (105) 2016. http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-553346c8-51f6-4d1f-8636-54a9a905dfdf/c/Milewski_Identyfikacja_infrastruktury.pdf (23.08.2018).

Pyznar, M., i inni (2014). *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, Instytut Kościuszki, Kraków. https://ik.org.pl/wp-content/uploads/bezpieczenstwo-infrastruktury-krytycznej-wymiar-teleinformatyczny_net.pdf (07.09.2018).

Rcb.gov.pl, (2018). *Infrastruktura Krytyczna*, https://rcb.gov.pl/infrastruktura-krytyczna/ (09.08.2018).

Rcb.gov.pl, (2018). *Narodowy Program Ochrony Infrastruktury Krytycznej*. http://www.rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%c5%82%c3%b3wny.pdf, 2013 (10.09.2018).

Szewczyk, T., Pyznar, M. (2010). *Ochrona infrastruktury krytycznej a zagrożenia asymetryczne*, Przegląd Bezpieczeństwa Wewnętrznego 2/2010. http://www.abw.gov.pl/download/1/1886/Szewczyk.pdf (07.08.2018 r.).

Tubielewicz, A., Forkiewicz, M. (2018) *Porty Morskie jako element infrastruktury krytycznej łańcucha dostaw,* Logistyka 2/2011, https://www.logistyka.net.pl/bank-wiedzy/transport-i-spedycja/item/download/74791_508e937e956b17b8530b05542aca9087 (23.08.2018).

Ustawa o ochronie żeglugi i portów morskich z dnia 4 września 2008 r (Dz. U. z 2018 r. poz. 435, 650). (07.09.2018).

Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz. U. 2018 r. poz. 1401, 1560). (07.09.2018).