bezpieczeństwo statku centrum monitoringu,
obieg i9nformacji,
monitoringu, zagrożenie

Artur CYWIŃSKI[1]
Dariusz SZULC[2]

KONCEPCJA CENTRUM OCHRONY I MONITORINGU PODWODNEGO PORTU MORSKIEGO

Rosnące znaczenie polskich portów morskich (zwłaszcza po wstąpieniu Polski do NATO) związane z ich położeniem oraz potencjalnymi możliwościami do zabezpieczenia różnego rodzaju działań militarnych, stwarza dla nich nowy rodzaj zagrożenia. Można oczekiwać pojawienia się prób wtargnięcia i penetracji na terenach portowych grup terrorystycznych, dywersyjnych oraz innych ukierunkowanych na różne wrogie działania. W artykule zaprezentowano rozwiązanie będące przykładowym modelem struktury centrum monitoringu basenów portowych i jako pewna koncepcja może w przyszłości okazać się przydatna. Wiele elementów tego modelowego rozwiązania już istnieje, a dodając do niego szereg nowych rozwiązań, z uwzględnieniem monitoringu podwodnego, model taki może być praktycznie wykorzystany i funkcjonować niemalże we wszystkich polskich portach.

THE CONCEPT OF HARBOUR' UNDERWATER PROTECTION AND MONITORING CENTRE

The growing meaning of Polish harbours (particularly after join the NATO Treaty) caused by their geographical location and potential possibilities to support the various kind of military actions is creating a new kind of threat for them. It can be expected to appear the attempts of intruding and/or penetrating the harbour area by terrorist or saboteur groups or other directed to various hostile actions. A solution being an example model of structure of monitoring centre of harbour's docks was presented in the following article and it can be use in the future as a reliable concept for further research. Many elements of such a model solution are existing already and adding to it a number of new solutions, with taking into consideration the underwater monitoring, such a model can be utilized in practice and serve in almost all Polish harbours.

[1] Akademia Marynarki Wojennej, Instytut Uzbrojenia Okrętowego, 81-103 Gdynia, ul. Śmidowicza 69, tel +48 58 626-28-74, e-mail: A.Cywiński@amw.gdynia.pl
[2] Akademia Marynarki Wojennej, Instytut Nawigacji i Hydrografii Morskiej, 81-103 Gdynia, ul. Śmidowicza 69, tel +48 58 626-29-50, e-mail: D.Szulc@amw.gdynia.pl

1. WSTĘP

Od końca XX wieku obserwuje się znaczny wzrost zagrożenia atakami terrorystycznymi skierowanymi na porty cywilne i wojenne oraz jednostki pływające. Z tego też względu przeciwstawienie się działaniom grup terrorystycznych jest jednym z podstawowych wyzwań, przed jakimi stoją państwa nadmorskie. Z tego względu wiele organizacji międzynarodowych podjęło prace legislacyjne, których celem jest podwyższenie poziomu bezpieczeństwa portów oraz cumujących w nich statków. Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26.10.2005 r. obliguje władze portów do wprowadzenia środków ochrony portów.

Do Konwencji SOLAS 74 przyjęto również rozdział XI-2 wprowadzający Kodeks ISPS[3] „Międzynarodowy kodeks ochrony statku i obiektu portowego" [1]. Głównym zamierzeniem Kodeksu ISPS było stworzenie zasad i procedur współpracy załóg statków i obiektów portowych w celu identyfikacji i przeciwdziałania źródłom zagrożeń bezpieczeństwa związanych z aktami terrorystycznymi w obszarze transportu morskiego. Wprowadzono poziomy bezpieczeństwa obowiązujące w portach jak również obowiązek stosowania urządzeń AIS (Automatic Identification System) dla jednostek pasażerskich, statków ro-ro, kontenerowców i tankowców.

Dlatego też, w celu zapewnienia bezpiecznej żeglugi w rejonach portów oraz postoju okrętów i statków w portach koniecznym jest opracowanie architektury systemu ochrony nawodnej i podwodnej infrastruktury portowej oraz utworzenie rozbudowanego systemu ochrony i monitoringu. Ochrona antyterrorystyczna okrętów, statków oraz infrastruktury portowej powinna być wspólnym zadaniem sił zbrojnych i agencji cywilnych. Dlatego niezbędna jest integracja oddzielnie istniejących systemów w jeden zintegrowany system ochrony antyterrorystycznej. Utworzona struktura powinna zapewniać między innymi wykrywanie celów stanowiących potencjalne zagrożenie, generowanie alarmów o wykrytych obiektach oraz niszczenie lub neutralizacje zagrożenia.

2. ARCHITEKTURA CENTRUM OCHRONY I MONITORINGU PORTU MORSKIEGO (COiMPM)

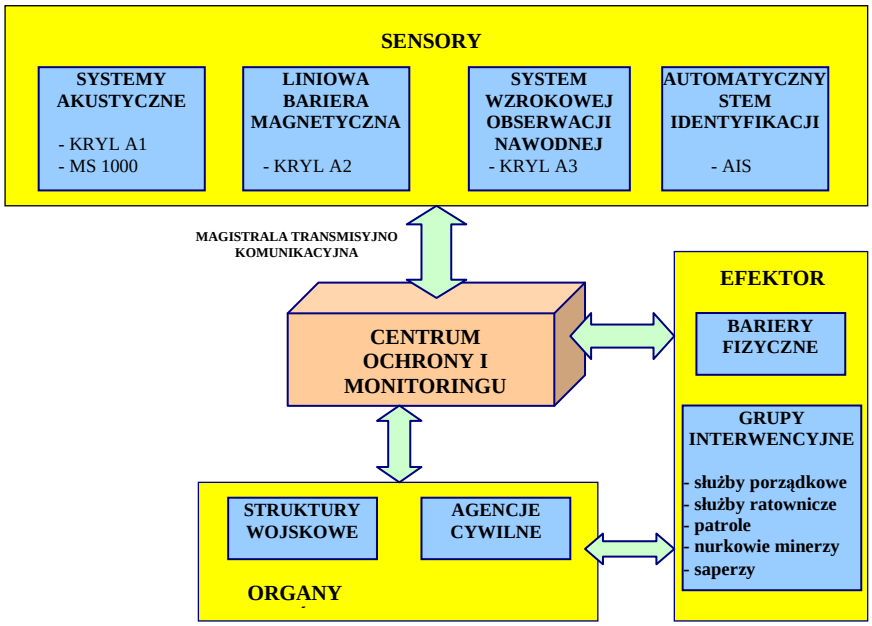
Rozbudowa sieci detektorów jak i współdziałanie pomiędzy różnymi komórkami zajmującymi się ochroną portu wymaga odpowiedniego zabezpieczenia logistycznego oraz działań koordynacyjnych. Dlatego też że konieczne jest utworzenie Centrum Ochrony i Monitoringu Portu Morskiego (COiMPM).

Utworzenie COiMPM umożliwi pełne wykorzystanie dostępnych środków technicznych wspomagających system ochrony. Co więcej ochrona antyterrorystyczna okrętów, statków oraz infrastruktury portowej jest wspólnym zadaniem sił zbrojnych i agencji cywilnych. Toteż COiMPM pełnić będzie rolę komórki integrującej oddzielnie działające systemy ochrony portów w zintegrowany system ochrony antyterrorystycznej.

Ze względu na fakt, że często Port Wojenny jak i Morski Port Handlowy sąsiadują ze sobą, koncepcja utworzenia COiMPM zapewniać powinna skuteczną ochrona tych rejonów angażując w to siły ochronnych Marynarki Wojennej i organów cywilnych.

[3]ISPS (International Code for the Security of Ship and of Port Facility).

Proponowany schemat systemu wzajemnych działań sił w ramach COiMPM przedstawia rys.1.



Rys.1. Schemat blokowy systemu wzajemnych działań sił w ramach COiMPM

Współpraca między wszystkimi kooperującymi ogniwami wojskowymi i cywilnymi powinna obejmować przede wszystkim wymianę informacji. Szczególnie ważne, ze względu na szybkie i skuteczne przeciwdziałanie powstałym zagrożeniom jest przekazywanie informacji w zakresie powiadamiania o pojawiających się symptomach zagrożenia oraz błyskawiczne reagowanie na powstałe zagrożenie i jego neutralizacja. Toteż COiMPM pełnić będzie rolę komórki nie tylko gromadzącej informacje, ale również koordynującej działania interwencyjne oraz zarządzającej dostępnymi środkami i siłami do ich realizacji. Zadania COiMPM obejmować powinny zatem:

- wykrywanie obiektów w bezpiecznej odległości od chronionych elementów lub obiektów pozostawionych na dnie;
- weryfikację wykrycia obiektu na kilku sensorach systemu (kilku kanałach);
- klasyfikację i identyfikację;
- alarmowanie;
- przesyłanie danych do stanowisk dowodzenia określonego szczebla (struktur wojskowych i agencji cywilnych);
- fizyczne zabezpieczanie dostępu do portu od strony morza;

- neutralizację wykrytych ładunków niebezpiecznych;
- obezwładnianie potencjalnych intruzów.

2. PODSYSTEMY WSPOMAGAJĄCE OCHRONĘ I MONITORING PORTU MORSKIEGO

Ważnym elementem mającym wpływ na bezpieczeństwo postoju statków w porcie ma kompleksowy system ochrony portu wraz z jego elementami zabezpieczeń. Elementy te to przede wszystkim zespół sensorów pasywnych i aktywnych zabezpieczających i chroniących przed niekontrolowanym dostępem do basenów portowych zarówno od strony lądu jak i morza. Dopełnienie systemu stanowić powinna nieprzerwana obserwacja całej infrastruktury portowej z jej obiektami, magazynami itp., która realizowana być powinna przez środki obserwacji technicznej – przemysłowe kamery telewizyjne czy kamery niskiego poziomu oświetlenia.

Rozpatrując jako przykład port gdyński, można stwierdzić, że położenie względem siebie Portu Wojennego i Morskiego Portu Handlowego wręcz narzuca konieczność budowy wspólnego systemu ochrony. Ze względu na specyfikę obu portów ich zadania co do ochrony obiektów i procedury, muszą pozostać niezależne i stanowić powinny autonomiczną część każdego z portów. Wiele jednak elementów związanych z ochroną można by przeprowadzać wspólnymi siłami co zwiększyłoby stopień bezpieczeństwa bez konieczności ponoszenia dodatkowych nakładów z każdej ze stron. Właściwym wydaję się w tej sytuacji wykonanie części zabezpieczeń siłami MW RP na rzecz Morskiego Portu Handlowego jak choćby bariery na wejście do portu.

Zagadnienie związane z tworzeniem bariery nie jest niczym nowym i ma już swoje rozwiązania aplikacyjne będące na wyposażeniu MW RP. Przykładem takiego rozwiązania jest system „Kryl'', który przeznaczony jest do detekcji celów podwodnych i nawodnych za pomocą sensorów hydroakustycznych, magnetycznych oraz optoelektronicznych. Zabezpiecza on ochraniany obiekt od strony morza tzn. pozwala na wykrywanie obiektów nawodnych i podwodnych zbliżających się do ochranianej strefy.

W skład systemu wchodzą:

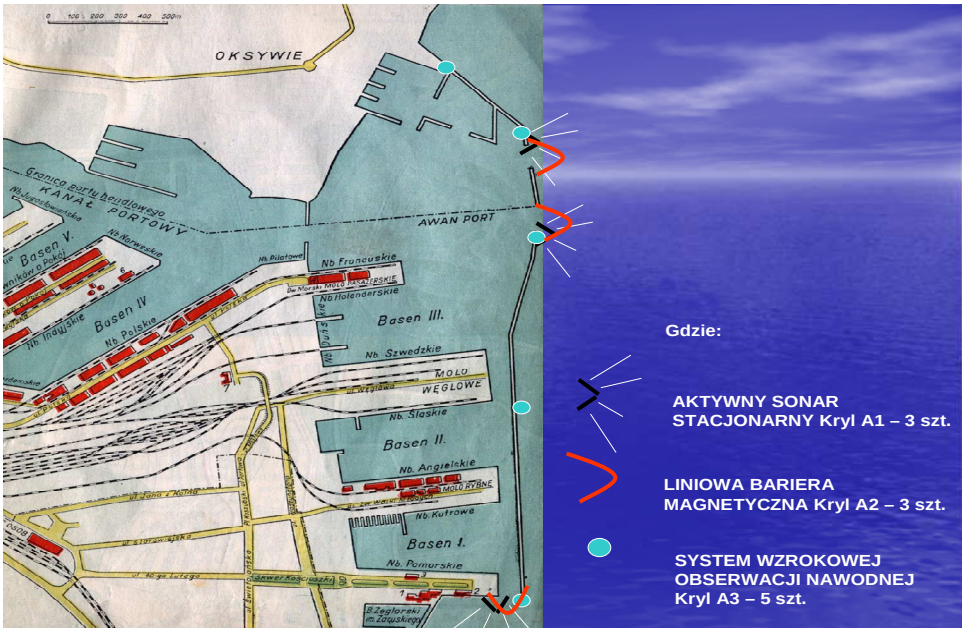
- podsystem Kryl A1 – aktywny sonar stacjonarny (ASS),
- podsystem Kryl A2 – liniowa bariera magnetyczna (MBL),
- podsystem Kryl A3 – wzrokowa obserwacja nawodna,
- podsystem Kryl B – pasywny system hydroakustyczny,
- podsystem Kryl C – komputerowe urządzenie sprzęgające (KUS),
- podsystem Kryl D – podsystem lotniczy,
- podsystem Kryl E – podsystem pomiaru pól fizycznych.

Wszystkie jednak urządzenia systemu „Kryl" są sensorami co sprawia, że wyłącznie informują o naruszeniu ochranianej strefy. Brak efektorów zabezpieczeń fizycznych jak bariery fizyczne neutralizujące zagrożenie czy profesjonalnie działające grup interwencyjno-patrolowe wyposażone w sprzęt specjalistyczny do neutralizacji ładunków wybuchowych. Brak jest również jasnych procedur określających sposób działania w konkretnych stanach zagrożenia terrorystycznego, a to stanowi o małym wykorzystaniu i małej przydatności całego systemu. Nieodzownym wydaje się w takiej sytuacji włączenie takiego systemu do schematu pracy w ramach przyszłego COiMPM, gdzie może się on stać

doskonałym narzędziem przydatnym w rozpoznawaniu i alarmowaniu o zagrożeniu ze strony morza.

System taki mógłby być dodatkowo wsparty o mobilny system monitoringu podwodnego, który w obecnym roku był testowany pod względem wykrywania ładunków niebezpiecznych zalegających na dnie w basenach portowych[4].

Proponowany sposób zabezpieczenia wejść do Portu Wojennego i Morskiego Portu Handlowego przedstawiono na rys. 2. Do zabezpieczenia zastosowano grupy sensorów radarowych, optoelektronicznych, magnetycznych oraz hydroakustycznych.



Rys.2. Proponowany sposób wykorzystania sensorów systemu „Kryl" na rzecz ochrony Portu Wojennego i Morskiego Portu Handlowego

2. ZOBRAZOWANIE INFORMACJI SYSEMÓW DETEKCJI

Podstawowym zadaniem systemu, którego przeznaczeniem będzie ochrona określonych obiektów powinno być ciągłe monitorowanie sytuacji nawodnej, podwodnej i terenów portu. Toteż wykryte, zlokalizowane i wstępnie sklasyfikowane zagrożenia powinny być zobrazowane w czasie rzeczywistym na zintegrowanej konsoli operatorskiej znajdującej się w Centrum Ochrony i Monitoringu Portu Morskiego.

Jako systemy obserwacji nawodnej i terenów portowych mogłyby być zastosowane podsystemy optoelektroniczne oparte na kamerach telewizyjnych i niskiego poziomu

[4] Projekt nr O N509 371034 pt. „System bezpiecznego postoju statku w porcie w warunkach zagrożenia terrorystycznego".

oświetlenia wspomagane systemami termowizyjnymi. Ich uzupełnienie stanowić powinna informacja pochodząca z Systemu Automatycznej Identyfikacji (AIS), który według zaleceń IMO i Międzynarodowych Przepisów o Zabezpieczeniu Statków i Portów (ISPS) powinien być zainstalowany na wszystkich statkach o pojemności brutto powyżej 300 DWT.

Nieco większy problem stanowi monitoring podwodny. Sonary aktywne pracujące w płytkich akwenach podejściowych do portów SA łatwo zakłócane i niezdolne do wykrywania małych obiektów pływających na powierzchni wody. Dlatego systemy obserwacji podwodnej powinny być wspomagane przez bariery magnetyczne oraz systemy obserwacji nawodnej w celu weryfikacji otrzymanej informacji. Nie bez znaczenia będzie tutaj wykorzystanie antyterrorystycznych, mobilnych systemów monitoringu podwodnego. W każdej wątpliwej sytuacji możliwe powinno być wykorzystanie, do sprawdzenia dna w newralgicznych miejscach portu, holowanych lub opuszczanych sonarów hydrograficznych.

Wszystkie uzyskane z powyższych informacje powinny spływać do Centrum i być wizualizowane na konsoli operatora. Zastosowane w niej rozwiązania techniczne powinny zapewniać:

- integrację wszystkich podsystemów (sensorów) na wspólnym zobrazowaniu sytuacji operacyjnej;
- przesyłanie danych do odpowiednich struktur decyzyjnych i wykonawczych;
- zdalne kierowanie i zarządzanie pracą wszystkich sensorów poprzez zunifikowaną magistralę transmisyjno-komunikacyjną;
- podgląd stanu i parametrów pracy poszczególnych podsystemów;
- klasyfikację nadzorowanych stref uwarunkowaną poziomem zagrożeń;
- automatyczne generowanie alarmu w oparciu o programowalne reguły i kryteria;
- ciągłą rejestrację zdarzeń (tras obiektów i danych) związaną z alarmowaniem o zagrożeniu w celu umożliwienia odtworzenia analizy sytuacji;
- elastyczność sprzętowo-programowej;
- zdalne wspomaganie i kierowanie w razie potrzeby grupami interwencyjnymi poprzez udzielanie informacji o zagrożeniu w czasie rzeczywistym.

4. PODSUMOWANIE

Podsumowując w celu zapewnienia bezpiecznej żeglugi w rejonie portów oraz postoju okrętów i statków w portach (Porcie Wojennym oraz Morskim Porcie Handlowym) nieuniknionym jest utworzeniu rozbudowanego systemu ochrony i monitoringu zapewniającego ochronę obiektów od strony lądu i morza. Utworzona struktura powinna zapewnić:

- wykrywanie celów stanowiących potencjalne zagrożenie;
- generowanie alarmów o wykrytych obiektach z bardzo małym prawdopodobieństwem alarmów fałszywych;
- niszczenie lub obezwładnienie potencjalnych intruzów.

Ponadto, zasadnym, a wręcz nieuniknionym wydaje się aby w tworzeniu ww. systemu partycypowały Marynarka Wojenna oraz organy cywilne w gestii których leży bezpieczeństwo żeglugi.

Utworzenie Centrum, w skład którego weszłyby nie tylko sensory, ale również efektory takie jak zabezpieczenia fizyczne czy bariery fizyczne i profesjonalne grupy interwencyjno-patrolowe jest czynnikiem priorytetowym i determinantem, pozwalającym na szybkie dostosowanie systemu ochrony do współczesnych niebezpieczeństw i zagrożeń.

W artykule przedstawiono jedynie zarys poruszanej tematyki. Znacznie szersze, kompleksowe opracowania z tego tematu były przedmiotem wielu prac prowadzonych w AMW. Szereg poruszanych tu problemów było przedmiotem licznych dyskusji i doczekał się wielu nowatorskich rozwiązań i wyczerpujących opracowań.

5. BIBLIOGRAFIA

[1] International Maritime Organisation: *International Ship & Port Facility Security Code and SOLAS Amendments 2002*, 2003.

[2] A. Cichocki, D. Szulc, *Stationary systems for underwater monitoring and traffic control on anchorages and approaches to ports. 10th International Conference „Computer systems aided science industry and transport" TRANSCOMP, Zakopane, 4-7.12.2006*

[3] D. Grabiec, D. Szulc, *System of antiterrorist attacks monitoring of sea bases and harbours VI-th International Armament Conference „Scientific aspects of armament technology" Waplewo, 11-13.10.2006*

[4] K. Kubiak, *Zagrożenie polskich obszarów morskich, Przegląd Morski 2001 nr 5*

[5] Cz. Dyrcz, *Terroryzm początku XXI wieku jako zagrożenie bezpieczeństwa międzynarodowego i narodowego, DMW, Gdynia 2005*