PRZEDSIĘBIORSTWO OCHRONY W PORTACH MORSKICH

Marcin FORKIEWICZ

Streszczenie: W pracy przeanalizowano obowiązujące wymogi prawne i organizacyjne w zakresie bezpieczeństwa portów i obiektów portowych, z uwzględnieniem wymagań ochrony infrastruktury krytycznej. Opisano organizację podstawowych działań, obowiązków i zadań w zakresie planowania i realizacji ochrony oraz zapewnienia gotowości na wypadek wystąpienia zdarzeń naruszających ochronę. Przedstawiono również przegląd nowoczesnych rozwiązań technologicznych, które mogą być wykorzystywane do zapewnienia odpowiedniego poziomu technicznej ochrony obiektów portowych.

Słowa kluczowe: porty morskie, bezpieczeństwo, przedsiębiorstwa ochrony, kodeks ISPS.

1. Wprowadzenie

Porty morskie stanowią złożone przestrzenne kompleksy gospodarcze, których działalność daleko wykracza poza ich granice administracyjne i silnie oddziałuje na procesy społeczno-gospodarcze w regionie. Na obszarze portu prowadzi działalność bardzo wiele różnych przedsiębiorstw oraz instytucji administracji państwowej, których aktywność gospodarcza związana jest z realizacją funkcji transportowej, przemysłowej, handlowej i logistycznej, jak również regionalnej portu.

Skomplikowana wielozakładowa struktura systemu portowo-przemysłowego oraz jego działalność na styku ląd-morze, jak i międzynarodowy charakter obrotów towarowych oraz ruchu pasażerskiego, powoduje że zagadnienia bezpieczeństwa w portach oraz ochrony portowych obiektów są jednym z najważniejszych problemów zarządzania strategicznego w portach morskich [1]. Czynnikami integrującymi port z przemysłem, usługami handlowymi i logistycznymi są kooperacja i współużytkowanie infrastruktury technicznej.

Porty morskie stanowią również ważne ogniwo w zintegrowanych morsko-lądowych łańcuchach transportowych, a tym samym w międzynarodowych łańcuchach dostaw (centra logistyczne). W morsko-lądowych łańcuchach transportowych logistyczne procesy integracyjne przebiegają pomiędzy trzema podstawowymi ogniwami: żeglugą morską, portami morskimi i transportem zaplecza, który odbywa się z wykorzystaniem pozostałych gałęzi transportu (drogowego, kolejowego, rurociągowego i wodnego śródlądowego) [2].

Zarządzanie kryzysowe w portach posiada charakter wysoce złożony o dużym stopniu skomplikowania i obejmuje wiele zróżnicowanych problemów przestrzennych, technicznych, ekonomicznych i społecznych [3]. W przypadku wystąpienia sytuacji kryzysowych, problemy te mogą stanowić poważne zagrożenie dla ekosystemu portowego oraz bezpieczeństwa społecznego w regionie. Szczególnie krytyczny charakter mogą mieć zakłócenia funkcjonowania łańcuchów dostaw oraz skażenia ekologiczne morza i przybrzeżnego środowiska naturalnego. Zdarzenia takie mogą wywołać długotrwałe skażenie akwenów portowych i terenów przyległych.

Wielorakie powiązania gospodarcze, przestrzenne i funkcjonalne pomiędzy portem a jego otoczeniem krajowym, regionalnym i miejskim powodują, że akweny i tereny portowe są szczególnie narażone na wystąpienie zdarzeń naruszających ochronę. Oceniając ryzyko i

konsekwencje potencjalnych zagrożeń należy uwzględniać zarówno bezpieczeństwo poszczególnych funkcji gospodarki portowej i ciągłość procesów biznesowych przedsiębiorstw portowych, ale także skutki przenoszone na otoczenie zewnętrzne portu, w tym ekologiczne, społeczne, ekonomiczne i transportowe w regionie.

Zapewnienie odpowiedniego poziomu bezpieczeństwa portów jest zagadnieniem skomplikowanym i wymaga zaangażowania administracji portowej i przedsiębiorstw zarządzających obiektami portowymi oraz profesjonalnego przygotowania i organizacji przedsiębiorstw ochrony portu. Zakres ochrony musi obejmować akweny i tereny portowe oraz związaną z nimi infrastrukturę techniczną, jak również ruch pasażerski, przepływ ładunków i środków transportu, obsługę statków morskich, itd.

2. Podstawy prawne działalności przedsiębiorstw ochrony w portach morskich

Zagadnienia bezpieczeństwa w portach morskich należy rozpatrywać z poziomu międzynarodowych, europejskich oraz krajowych aktów prawnych:

1. Międzynarodowego kodeks ochrony statku i obiektu portowego – Kodeks ISPS [4], Międzynarodowej Organizacji Morskiej – IMO (2002 r.);
2. Dyrektywy Parlamentu Europejskiego i Rady w sprawie wzmocnienia ochrony portów (2005 r.) [5];
3. Dyrektywy Rady w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony (2008 r.) [6];
4. Ustawy o ochronie żeglugi i portów morskich (2008 r.) [7];
5. Ustawy o zarządzaniu kryzysowym (2007 r., nowelizacja 2009 r.) [8].

Natomiast przedsiębiorstwa i służby ochrony portu muszą działać zgodnie z ustawą o ochronie osób i mienia [9] oraz ustawą o broni i amunicji [10].

Kodeks ISPS [4] jest zbiorem wymagań w zakresie sił i środków ochrony, a także procedur prewencyjnych i wytycznych, które mają służyć wzmocnieniu ochrony żeglugi oraz zapobiegać ewentualnym próbom przeprowadzenia ataków terrorystycznych na statki i obiekty portowe. Dyrektywa w sprawie wzmocnienia ochrony portów [5] oraz ustawa o ochronie żeglugi i portów morskich [7] są aktami prawnymi wdrażającymi zasady kodeksu ISPS w prawie europejskim i krajowym.

Zgodnie z kodeksem ISPS, obiektem portowym jest obszar portu lub przystani, w którym zachodzą relacje statek/port. Dla każdego obiektu portowego kodeks nakłada następujące główne wymagania [2]:

1. obowiązek stosowania trzech poziomów ochrony obiektów (podstawowego, podwyższonego i wysokiego);
2. przeprowadzenie oceny stanu ochrony obiektu, zawierającej ocenę ryzyka i zagrożeń dla ochrony obiektu oraz ciągłości prowadzonej w nim działalności;
3. stworzenie planu ochrony obiektu – na podstawie oceny stanu ochrony obiektu – który będzie zawierać odpowiednie środki ochrony (przeciwdziałania) dla każdego z trzech poziomów ochrony;
4. wyznaczenie odpowiednio wykwalifikowanej (zgodne ze standardami IMO) osoby odpowiedzialnej za opracowanie i realizację postanowień planów ochrony – tzw. oficera ochrony obiektu portowego;
5. przeprowadzanie regularnych szkoleń i ćwiczeń związanych z ochroną obiektu.

Również musi zostać wyznaczony oficer ochrony portu, a na podstawie oceny stanu ochrony portu oraz planów ochrony poszczególnych obiektów portowych stworzony powinien zostać zintegrowany planu ochrony portu jako kompleksu.

Zarządzanie kryzysowe w portach morskich [3] oznacza działalność organów administracji terytorialnej [11] oraz morskiej (urzędy morskie) i portowej (zarządy portów) w zakresie zapobiegania sytuacjom kryzysowym, przygotowania do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowania w przypadku wystąpienia sytuacji kryzysowej, usuwania ich skutków oraz odtwarzania zasobów i infrastruktury krytycznej.

Portową infrastrukturą krytyczną [6] jest lądowa i wodna (w tym nawigacyjna) infrastruktura techniczna wchodząca w skład morsko-lądowego systemu transportowego i komunikacyjnego oraz występujące w portach systemy łączności, przeładunku, składowania, przechowywania materiałów i substancji niebezpiecznych, sieci teleinformatyczne oraz systemy ratownictwa [2].

Ochrona portowej infrastruktury krytycznej obejmuje działania zmierzające do zapewnienia funkcjonalności, ciągłości i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie [8].

Ocena stanu ochrony portu i obiektów portowych [12] powinna uwzględniać możliwe scenariusze zdarzeń naruszających ochronę – potencjalnych, zamierzonych, bezprawnych ataków na port, obiekt portowy, urządzenia, statki i infrastrukturę krytyczną, ze strony lądu, powietrza, wody i spod wody. Należy też określić ryzyko zdarzeń zagrażających bezpieczeństwu jako zależność prognozowanych konsekwencji i prawdopodobieństwa zajścia zdarzenia. Stanowi to podstawę identyfikacji zdarzeń, które wymagają zastosowaniu skutecznych operacyjnych i/lub fizycznych środków zaradczych, mających na celu zredukowanie ryzyka do akceptowalnego poziomu.

Planowanie ochrony portu i jego obiektów [13] obejmuje określanie organizacji w zakresie bezpieczeństwa portu, podziału zadań, procedur roboczych, zasad koordynacji z oficerami bezpieczeństwa oraz komunikacji z organami i służbami odpowiedzialnymi za bezpieczeństwo w porcie, jak również organizację szkoleń i ćwiczeń w tym zakresie.

Plan ochrony obiektu portowego [2] powinien być opracowany na postawie oceny stanu każdego obiektu portowego, adekwatnie do relacji statek/port oraz oceny zagrożeń określającej najbardziej prawdopodobne rodzaje wypadków (zagrożeń i scenariuszy), w odniesieniu do każdego wyszczególnionego elementu obiektu portowego, wymagającego ochrony, szczególnie w zakresie elementów infrastruktury krytycznej.

Plan ochrony powinien być tworzony przez podmiot całkowicie niezależny od późniejszego wykonawcy samej ochrony i traktowany jako dokument niejawny. W przypadku obiektów podlegających obowiązkowej ochronie (porty morskie) plan ochrony musi zostać uzgodnionym z odpowiednim terytorialnie komendantem policji. Plany ochrony portu i obiektów portowych musi być w pełni zgodne z zasadami kodeksu ISPS.

3. Zakres ochrony portów morskich realizowany przez przedsiębiorstwa ochrony

Bezpieczna praca portów oraz powiązanych z nim zakładów produkcyjnych i usługowych (np. stoczni produkcyjnych i remontowych) wymaga szerszego zaangażowania podmiotowego i przedmiotowego [3]. Oznacza to konieczność poszerzenia zakresu podmiotów wpływających na poziom bezpieczeństwa w porcie oraz rozszerzenia zakresu ochrony, jej zasięgu przestrzennego oraz wykorzystywanych metod i środków.

Duża skala zagrożeń bezpieczeństwa w portach morskich wynika m.in. z:

– międzynarodowego charakteru działalności portu;

- funkcjonowania portu na styku dwóch środowisk: morza i lądu;
- znaczenia portów w systemie gospodarki narodowej;
- roli portów w morsko-lądowych łańcuchach transportowych (łańcuchach dostaw);
- skoncentrowania majątku o dużej wartości na obszarze portu (środków trwałych, wyposażenia i ładunków);
- dużej dynamiki przepływu ludzi i ładunków pochodzących z różnych źródeł;
- obecności przedstawicielu wielu przedsiębiorstw oraz rezydentów państw obcych;
- powiązań gospodarczych, transportowych, przestrzennych i społecznych portu z jego otoczeniem lokalnym, regionalnym i krajowym.

Potencjalne zagrożenie bezpieczeństwa stanowią m.in. zdarzenia i ich konsekwencje:

- zdarzenia spowodowane siłami natury;
- ataki terrorystyczne;
- katastrofy ekologiczne;
- pożary i wycieki substancji szkodliwych;
- kradzieże i włamania;
- przemyt ludzi, ładunków i substancji niebezpiecznych;
- skażenie transportowanych artykułów spożywczych;
- sabotaż gospodarczy lub polityczny.

Port morski jest obiektem podlegającym obowiązkowej ochronie zgodnie z ustawą o ochronie osób i mienia [9] i jako taki musi być chroniony przez specjalistyczne uzbrojone formacje ochronne (sufo). Przedsiębiorstwo ochrony musi posiadać odpowiednią koncesję MSWiA do prowadzenie działalności gospodarczej w zakresie ochrony osób i mienia oraz pozwolenie na broń na okaziciela (tj. świadectwo broni) wydane zgodnie z ustawą o broni i amunicji [10]. Dodatkowo ochrona musi być zorganizowana zgodnie z ustawą o ochronie żeglugi i portów morskich [7] oraz ustawy o zarządzaniu kryzysowym w zakresie ochrony portowej infrastruktury krytycznej [8]. Ustawa o ochronie osób i mienia [9] nakazuje też uzgadniać plany ochrony z właściwym terytorialnie komendantem wojewódzkim policji.

Ochrona portu może być także realizowana przez wewnętrzne służby ochrony, tzn. uzbrojone i umundurowane zespoły pracowników przedsiębiorstwa powołane do ochrony [9] – „staż portową". W obu przypadkach zadania ochrony osób i mienia mogą być wykonywane tylko przez pracowników posiadających odpowiednie licencje: pracownika ochrony fizycznej lub pracownika zabezpieczenia technicznego (licencje I i II stopnia) [11].

Outsourcing usług ochrony polega na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa macierzystego (zarządu portu) realizowanych funkcji związanych z bezpieczeństwem i ochroną oraz przekazaniu ich do realizacji specjalizującym się w tym zakresie podmiotom gospodarczym. Dzięki temu może się ono skoncentrować na działalności strategicznej, zachowując skuteczną kontrolę wydzielonych procesów.

Należy przy tym zaznaczyć, że nie można bezpieczeństwa portu ograniczać wyłącznie do prostych usług ochrony, gdyż działania w tym zakresie wymagają specjalistycznej wiedzy i odpowiedzialności realizującego je podmiotu. Zakres działania jednostek ochrony portu musi być dostosowany do realnych zagrożeń i warunków otoczenia oraz podlegać ciągłej modyfikacji ze względu na pojawiające się nowe niezidentyfikowane rodzaje zagrożeń oraz wzrost przestępczości indywidualnej i zorganizowanej.

W przedsiębiorstwie portowym ochrona powinna dotyczyć przede wszystkim trwałych wartości decydujących o istnieniu i funkcjonowaniu firmy [14]:

- ludzie (goście i pracownicy wraz z ich potencjałem intelektualnym);
- rzeczy materialne (teren, budynki, środki pieniężne, majątek trwały i ruchomy);

– informacje/dane (własne i powierzone, w tym dane osobowe);
– elementy infrastruktury zewnętrznej, szczególnie infrastruktury krytycznej.

Podstawowe cele działalności przedsiębiorstwa ochrony świadczącego usługi na rzecz zarządu portu można określić następująco:

– zapewnienie bezpieczeństwa portu;
– zapobieganie nieupoważnionemu dostępowi do obszaru strzeżonego portu;
– przeciwdziałanie zagrożeniom lub zdarzeniom naruszającym ochronę.

Natomiast główne zadania polegają na:

– regulacji ruchu osobowego, samochodowego, materiałowego;
– zabezpieczeniu rejonów portu stale lub czasowo strzeżonych;
– zapobieganiu nielegalnemu wniesieniu/wwiezieniu na obszar portu broni, materiałów wybuchowych i innych materiałów niebezpiecznych.

4. Organizacja ochrony portów morskich przez przedsiębiorstwa ochrony

Realizacja bezpieczeństwa fizycznego w wymaga realizowania trzech podstawowych czynności ochronnych, które muszą być odzwierciedlone w strukturze organizacyjnej [14]:

– strefowania (strefy: jawna, ograniczona, zamknięta);
– dostępność (ogólna dostępność i strefy wydzielone);
– dozorowania zasobów przedsiębiorstwa: wartości, ludzi i informacji.

Teren portu morskiego zwykle podzielony jest na dwie części: część otwartą (ogólnodostępną) z systemem komunikacji miejskiej i dróg publicznych oraz część zamkniętą chronioną przez wyspecjalizowane służby ochrony. Konieczność zamknięcia części terenów portowych oraz wprowadzenie środków ochrony fizycznej i zabezpieczenia technicznego obiektów portowych wynika z realizacji zasad kodeksu ISPS.

Organizacja ochrony fizycznej opiera się na tworzeniu lub wykorzystaniu istniejących barier materialnych i technicznych (np. murów, ogrodzeń) do postaci stałego nadzorowania obwodu ochrony fizycznej [14]. Utworzenie obwodu ochrony fizycznej oznacza ograniczenie dostępu do niego oraz wymaga opracowania precyzyjnego planu ochrony z uwzględnieniem procedur organizacyjnych, ochronnych i technicznych.

Podstawowy zakres działań przedsiębiorstwa ochrony portu obejmuje:

– ochronę obszarów, obiektów portowych, budynków i urządzeń podlegających ochronie obowiązkowej zgodnie z ustawą o ochronie osób i mienia;
– ochronę obiektów, budynków i mienia, nie podlegających obowiązkowej ochronie, w zakresie ustalonym przez zarząd portu lub operatorów terminali;
– ochronę obiektów portowych zgodnie z wymogami kodeksu ISPS oraz ustawy o ochronie żeglugi i portów morskich.

Specjalistyczne przedsiębiorstwo ochrony portu morskiego (o charakterze sufo), spełniające opisane wcześniej wymogi formalno-prawne, musi dysponować zatrudnionymi pracownikami, którzy spełniają w szczególności następujące warunki:

– posiadają licencję pracownika ochrony fizycznej pierwszego/drugiego stopnia;
– ukończyli szkolenie w zakresie kodeksu ISPS;
– posiadają potwierdzenie legalności posiadania broni przez pracownika ochrony fizycznej (wpis w legitymacji osoby dopuszczonej do posiadania broni);
– nie zostali skazani prawomocnym wyrokiem za przestępstwo umyślne;

w liczbie odpowiedniej do specyfiki i wielkości chronionych obiektów i obszarów (terenów i akwenów) portowych.

W zakresie potencjału technicznego przedsiębiorstwo ochrony powinno posiadać: oznakowane samochody patrolowe, broń palną bojową krótką, paralizatory elektryczne, środki przymusu bezpośredniego, środki łączności bezprzewodowej, lornetki noktowizyjne, latarki halogenowe oraz jednolite umundurowanie pracowników w sposób umożliwiający ich identyfikację. Zazwyczaj od przedsiębiorstwa jest wymagane również posiadanie ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności.

Ochrona portu i obiektów portowych jest realizowana przez:

- stałe posterunki całodobowe na bramach portowych;
- całodobowe patrole zmotoryzowane (dwuosobowe);
- fizyczny dozór wybranych obiektów (obsługa jednoosobowa portierni);
- obsługę stacji monitorowania alarmów i monitoringu wizyjnego;
- ochronę elektroniczną wybranych obiektów i pomieszczeń;
- prowadzenie systemu przepustek osobowych, samochodowych i materiałowych, uprawniających do wejścia i wjazdu na chronione obszary;
- posterunki wartownicze i patrole piesze (wystawiane w związku z zawinięciem statków pasażerskich lub wprowadzeniem wyższego poziomu ochrony).

Wśród zadań i obowiązków pracowników przedsiębiorstwa ochrony (wartowników) można wyróżnić:

- współdziałanie z oficerem ochrony portu i oficerami ochrony poszczególnych obiektów portowych;
- ochrona Kapitanatu Portu;
- kontrolę dostępu (np. do nabrzeży) osób i pojazdów;
- regulowanie ruchem pojazdów na nabrzeżu;
- zezwalanie na wjazd pojazdów i ładunków bezpośrednio związanych ze świadczonymi usługami;
- zapewnienie porządku publicznego na ochranianym obszarze (dostępnym np. dla firm przewozowych osób i ładunków);
- ochronę obszarów o tymczasowo ograniczonym dostępnie (np. wzdłuż burty statku pasażerskiego) oraz podejmowanie interwencji w przypadku naruszenia ochrony;
- kontrolowanie uprawnień do wstępu lub wjazdu na teren strzeżony;
- stałe sprawdzanie stanu zabezpieczeń obiektów oraz nabrzeży;
- kontrolę osób, środków transportu i towarów w celu sprawdzenia czy mienie nie jest bezprawnie wynoszone lub wywożone;
- w uzasadnionych przypadkach ujęcie sprawcy włamania, kradzieży lub innego czynu zabronionego i niezwłoczne przekazanie policji;
- w sytuacjach zagrożenia podjęcie bezzwłocznej interwencji zmierzającej do zapobieżenia szkodzie lub jej ograniczenia.

Ponadto przedsiębiorstwo ochrony musi być gotowe do wzmocnienia ochrony oraz wystawienia dodatkowych posterunków i patroli wartowniczych w przypadku wprowadzenie przez oficera ochrony portu wyższego poziomu ochrony w całym porcie lub poszczególnych obiektach portowych. Ćwiczenia sprawdzające w tym zakresie muszą się odbywać zgodnie z planem ochrony portu oraz planami ochrony poszczególnym obiektów portowych, zgodnie z wymogami kodeksu ISPS.

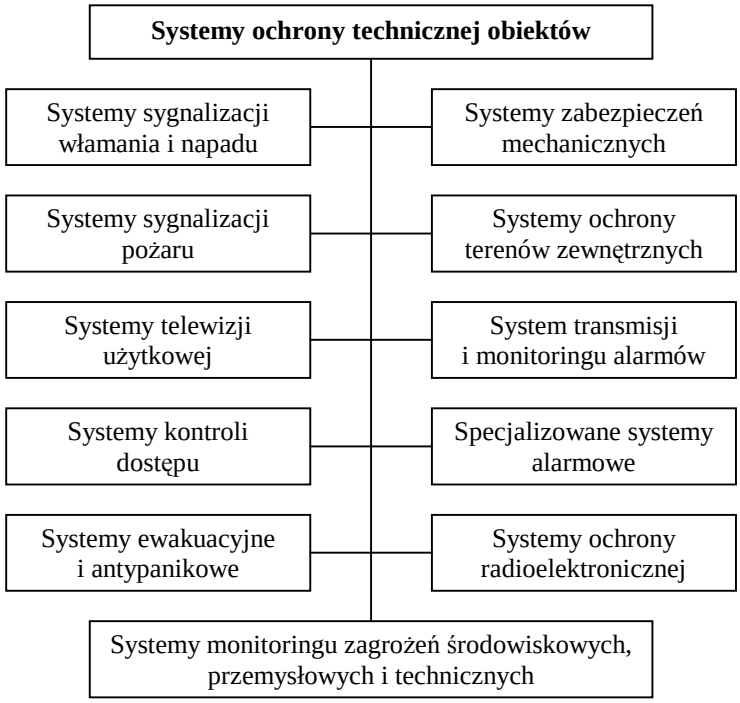
Skuteczna realizacja zadań związanych z ochroną portu wymaga także ścisłej współpracy z instytucjami i służbami odpowiedzialnych za bezpieczeństwo jak np.: policja, straż graniczna, straż pożarna, służba celna, urzędy morskie, służby specjalne, itd. [11].

5. Systemy ochrony technicznej w portach morskich

Skuteczność systemów ochrony określa triada bezpieczeństwa [15], która wskazuje na współdziałanie trzech czynników bezpiecznego funkcjonowania przedsiębiorstwa:

- systemu ochrony technicznej – obejmującego urządzenia i środki zabezpieczenia mechanicznego oraz elektroniczne urządzania i systemy alarmowe;
- systemu ochrony fizycznej – realizowanego przez pracowników ochrony, obejmującego również czynności interwencyjne w przypadku alarmu;
- organizacji funkcjonalnej przedsiębiorstwa, w tym zasad działania sytemu ochrony, z uwzględnieniem zagadnień kultury bezpieczeństwa [16].

Rozwój technologii informatycznych (programowych i sprzętowych), miniaturyzacja urządzeń oraz zwiększenie niezawodności powodują, że wzrasta ich wykorzystanie w ochronie mienia, obiektów i obszarów. Projektowanie i instalowanie systemów ochrony technicznej (rys. 1) wymaga poszukiwania kompromisu pomiędzy możliwościami technicznymi urządzeń, a potrzebami zapewnienia bezpieczeństwa – pomiędzy rzeczywistą skutecznością a kosztami inwestycyjnymi i eksploatacyjnymi.



Rys. 1. Systemy i podsystemy ochrony technicznej obiektu
Źródło: Wójcik A.: Materiały szkoleniowe ES INSTAL, Warszawa–Katowice, 2004 [14].

Warto zaznaczyć, że w rozwiązaniach praktycznych należy stosować uzasadnioną ekonomicznie i technicznie kombinację urządzeń elektronicznych, systemów komputerowych i sieciowych oraz oprogramowania, dzięki którym otrzymany zostanie

pożądany poziom ochrony, adekwatny do ryzyka związanego z potencjalnymi zagrożeniami naruszającymi ochronę, przy akceptowalnym poziomie niezawodności.

W praktyce określając granice ochrony technicznej obiektu wykorzystuje się istniejącą infrastrukturę materialną (mury, okna). System ochrony obiektu oparty jest na rozwiązaniach organizacyjnych oraz wspierany środkami technicznymi (rys. 1). Wysokość kosztów ochrony (szczególnie wynikającej z wymagań ustawowych) powoduje, że często wydziela się w obiektach obszary bezpieczeństwa o rożnym poziomie ochrony.

Poniżej przedstawiono przegląd dostępnych na rynku rozwiązań technologicznych (na podstawie przeprowadzonych badań własnych), które mogą zostać wykorzystane w projektowaniu technicznych systemów ochrony portów morskich (akwenów i terenów). W opisie skoncentrowano się na zestawieniu funkcjonalności i podstawowych cech urządzeń i systemów elektronicznych, a nie szczegółowych parametrów i charakterystyk technicznych konkretnych urządzeń oferowanych przez producentów.

Systemy monitoringu wizyjnego (telewizji dozorowej – ang. *Close Circuit Television* – CCTV) służą do obserwacji i rejestracji obrazu. Dzielone są na: obserwacyjne, detekcyjne (detekcja ruchu), inteligentne (analiza zmian w scenerii otoczenia) i sieciowe (z wykorzystaniem sieci IP). Najbardziej dynamicznie rozwijanym produktem są kamery, których producenci oferują następujące cechy użytkowe: szybkoobrotowość, wysoką rozdzielczość, tryb dzień/noc, zmienno-ogniskowy obiektyw (kilkunastokrotny zoom optyczny), zastosowanie wewnętrzne i zewnętrzne (z pogrzewaczami, odporne na warunki atmosferyczne, zagrożenie wybuchem i środowiska agresywne), systemy termowizyjne (detekcja promieniowania elektromagnetycznego – IR) oraz systemy noktowizyjne.

Centra obsługi monitoringu (nadzoru) wyposażane są w wielokanałowe rejestratory cyfrowe i serwery wideo (pracujące również w sieci IP) oraz aplikacje do analizy obrazu z kamer monitorujących (także w czasie rzeczywistym). W nowoczesnych typach oprogramowania do nadzoru realizowane są funkcjonalności:

- diagnostyka poprawności działania urządzeń monitorujących (np. kamer);
- identyfikacja obiektów ruchomych i statycznych;
- identyfikacja kolorystyki obiektu i tekstury tła;
- analiza zachowań tłumu;
- kierunkowa detekcja ruchu i pozycjonowanie na mapie;
- detekcja zdefiniowanych ruchów (np. upadek, rzucenie przedmiotu) i obiektów (np. pies, bagaż, człowiek);
- rozpoznawanie ludzkich twarzy i przedmiotów (np. samochodów, tablic rejestracyjnych).

Systemy ochrony obszarowej wykorzystywane są najczęściej w ochronie dużych terenów otwartych np. parkingów, terminali, stacji energetycznych, lotnisk. Celem ich stosowania jest rejestracja przekroczenia przez potencjalnego intruza barier ochronnych – fizycznych lub elektronicznych. Systemy wyposaża się w urządzenia, takie jak:

- czujniki ruchu, w tym z detekcją podczerwieni, mikrofal, ultradźwięków;
- bariery wielowiązkowe (mikrofalowe, podczerwieni);
- czujniki hydrauliczne (wykrywanie różnicy ciśnienia – np. nacisku);
- ochronę obwodową – kable sensoryczne (napłotowe lub zakopywane);
- laserowe czujniki dystansu;
- detektory ruchu (kierunkowe czujki kurtynowe);
- mikrofony przemysłowe;
- radary nadzorujące z funkcją określania położenia intruza.

W praktyce warto sprzęgać systemy ochrony obszarów z systemami monitoringu wizyjnego, poprzez nakierowywanie kamer na miejsca naruszenia ochrony lub potencjalne kierunki pojawienia się intruza w bliższej odległości od obiektu chronionego.

Systemy sygnalizacji włamań i napadów budowane są z sieci czujników wykrywających i sygnalizujących włamanie lub próbę wtargnięcia oraz centrali alarmowej (połączonej przewodowo lub z transmisją sieciową) przekazującej sygnał operatorowi. Wśród urządzeń detekcyjnych można wyróżnić:

- czujki ruchu – podczerwieni IR (wykrywanie temperatury różnej od otoczenia);
- czujki ruchu – mikrofalowe (oraz czujniki dualne wraz z czujnikiem IR);
- czujki magnetyczne (tzw. kontaktrony) – zabezpieczenie wszelkich elementów zamykających otwory w ścianach i meblach;
- czujki mikrofonowe – reagowanie na np. dźwięk tłuczonego szkła (zwykłego, hartowanego, zbrojonego, oklejanego, itp.);
- czujki wibracyjne – wykrywanie drgań powierzchni, na której zostały zamontowane (np. bicia szkła);
- czujki ochrony obwodowej – bezprzewodowe bariery podczerwieni.

Czujki mogą posiadać zabezpieczenia antysabotażowe (np. oderwanie, zasłonięcie, przerwanie zasilania).

Systemy identyfikacji i kontroli dostępu służą do elektronicznej kontroli dostępu osób wchodzących i wychodzących z obiektu. Mogą również rejestrować obecność i czas przebywania oraz historię osób przebywających w obiektach. Identyfikacja i kontrola „tożsamości" ludzi odbywa się z wykorzystaniem:

- czytników kodu numerycznego (PIN kodu);
- czytników elektronicznych kart identyfikacyjnych z kodem danej osoby lub pojazdu (kart zbliżeniowych);
- czytników cech biometrycznych (linii papilarnych, kształtu dłoni, tęczówki oka, rysów twarzy, odcisku palca, skanery skóry wewnętrznej, sensory biometrii żył);
- optycznych czytników dokumentów (dowodów osobistych, praw jazdy, europejskich kart ubezpieczenia zdrowotnego, kart biznesowych);
- czujników opartych na pomiarze pola magnetycznego (dostęp do gablot, szuflad);
- systemu monitorowania i depozytorów kluczy (rejestrowanie wyjmowania i wkładania nośników kluczy).

Systemy sygnalizacji pożarowej (monitoring pożarowy) obejmują urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych. Zadaniem systemów jest wczesne wykrycie pożaru i wskazanie miejsca jego powstania oraz powiadomienie o niebezpieczeństwie personelu (oraz np. straży pożarnej).

Centrale sygnalizacji pożarowej (centrale alarmowe) gromadzą, przetwarzają (analizują) i wizualizują sygnały przesyłane przez urządzenia detekcji oraz wysyłają sygnały alarmowe do urządzeń odbiorczych. Mogą również sterować urządzeniami wykonawczymi do gaszenia pożaru, a także:

- sygnalizatorami: optycznymi, akustycznymi, optyczno-akustycznymi (od syreny do wyświetlacza tekstu alarmowego);
- zaworami (klapowymi i motylowymi), drzwiami, oknami i grodziami ppoż.;
- urządzeniami automatyki oddymiania i napowietrzania, wyłączania energii elektrycznej, włączania wentylatorów, kierowania ewakuacją, itd.

Wśród urządzeń detekcji można wyróżnić czujki: płomieni (reagujące na promieniowanie podczerwone), termiczne (wykrywające zmiany temperatury) oraz zadymienia (analizujące optycznie rozproszenie światła przez dym w różnych barwach).

Stosowane są również wielosensorowe czujki dymu, wyposażone dodatkowo w detektory gazów – np. wielodetektorowa czujka dymu z detektorami optycznym i termicznym. Dodatkowo do identyfikacji pożarów można wykorzystywać kamery termowizyjne rejestrujące np. źródła ognia, wybuchy.

Urządzenia do detekcji i rozpoznawania gazów niebezpiecznych są szczególnie pomocne w przypadku wystąpienia zagrożenia pożarem, wybuchem, katastrofą ekologiczną i atakiem terrorystycznym. Detektory można podzielić na następujące grupy:

- detektory i identyfikatory substancji radioaktywnych (detekcja podwyższonego poziomu radioaktywności, podział na izotopy: bezpieczne, podejrzane i groźne);
- detektory i identyfikatory gazu ziemnego i LPG (propan butan) i produktów ich spalania oraz wycieku środków chłodniczych;
- detektory i identyfikatory gazów łatwopalnych, wybuchowych i toksycznych (O_2, H_2S, CO, CO_2, SO_2, H_2S, CO, NH_3, HCN, NO_2, PH_3, Cl_2) oraz niedoboru tlenu;
- detektory i identyfikatory materiałów wybuchowych, toksycznych środków przemysłowych, bojowych środków chemicznych, narkotyków, itp.

W praktycznych zastosowaniach występują detektory jedno- lub wielogazowe. Stosowane są również urządzenia sygnalizacyjno-odcinające, w których system detekcji gazu sprzężony jest z zaworem odcinającym.

Systemy kontroli ruchu (ang. *Traffic System Control* – TSC) – obejmują kontrolę ruchu w zakresie: osób, samochodów osobowych, pojazdów ciężarowych, pojazdów szynowych. Systemy posiadają funkcje:

- kontroli wjazdu i wyjazdu (na podstawie odczytu danych z tablic rejestracyjnych);
- automatycznego pomiaru masy, nacisków na osie oraz wymiarów pojazdu (z wykorzystaniem odpowiednich zewnętrznych urządzeń pomiarowych);
- automatycznego odczytu numerów kodów kontenerów i cystern (z wykorzystaniem kamery liniowej);
- lokalizacji pojazdów z wykorzystaniem systemu GPS.

Sterowalne oświetlenie dla systemów monitorowania i dozoru. Właściwy dozór i monitoring przestrzeni wymaga odpowiedniego oświetlenia. Stałe oświetlenie (przy braku naturalnych źródeł światła) powierzchni i obiektów chronionych, szczególnie na zewnątrz budynków, powoduje duże koszty. Oświetlenie dużych przestrzeni powinno być sterowalne, tzn. uruchamiane na przykład wcześniej opisanymi detektorami ruchu lub wtargnięcia intruza, z jednoczesnym skierowaniem wiązki świetlnej na miejsca najbardziej zagrożone. Wśród urządzeń oświetleniowych warto wyróżnić: promienniki podczerwieni i (widocznego) światła białego oraz diody LED.

Stacje meteorologiczne. W przypadku wystąpienia pożaru, skażenia biologicznego, promieniotwórczego bądź chemicznego bardzo ważne jest szybkie opracowanie modelu rozprzestrzeniania się zanieczyszczeń. Niezbędne do tego jest specjalistyczne oprogramowanie działające w oparciu o aktualizowane na bieżąco specjalne bazy danych substancji niebezpiecznych i ich możliwych interakcji oraz scenariuszy rozprzestrzeniania skażenia. Kluczowym elementem tego systemu są stacje meteorologiczne (pogodowe) – stacjonarne i mobilne (przenośne).

Mobilne stacje meteorologiczne posiadają elektroniczny kompas, dokładnie orientujący położenie stacji po jej rozłożeniu na specjalnym maszcie. Stacje wyposażane są w komplet czujników umożliwiających oszacowanie kierunku i dynamiki rozprzestrzeniania się

pożaru i/lub zagrożenia chemicznego. Wśród nich można wyróżnić czujniki: temperatury, wilgotności względnej, ciśnienia atmosferycznego, opadów, prędkości i kierunku wiatru oraz promieniowania jądrowego. Parametry rejestrowane oraz wyliczane (np. temperatura punktu rosy, temperatura odczuwalna) wyświetlane są na wyświetlaczu LCD lub wyświetlaczu z użyciem diod LED, który charakteryzuje się większą czytelnością.

Systemy zintegrowane łączą w sobie cechy różnych systemów ochrony, które stanowią bazę integracji. Wyposażone są w centrum alarmowe (monitoringu, ochrony przeciwpożarowej i koordynacji działań) oraz system informatyczny łączący w sobie funkcjonalności opisanych powyżej systemów. Centrala komputerowa rejestruje i przetwarza sygnały pochodzące od urządzeń wejściowych (czujników, detektorów, rejestratorów, itp.) oraz na bazie zaimplementowanych procedur i scenariuszy realizuje określone sekwencje działań zarządzania kryzysowego.

Techniczne systemy ochrony – wykorzystujące urządzenia elektroniczne powinny być wyposażone także w systemy:

- bezpiecznego zasilania (z układem awaryjnego podtrzymania zasilania);
- bezpiecznej transmisji informacji drogą elektroniczną (w tym bezprzewodowo);
- bezpieczeństwa infrastruktury informatycznej i danych.

6. Podsumowanie

Przedsiębiorstwo ochrony portu morskiego (jako specjalistyczna uzbrojona formacja ochronna) musi spełniać wszystkie formalne wymogi potwierdzone uzyskanymi: koncesją, pozwoleniami oraz świadectwami ukończonych szkoleń. Jednakże skuteczna realizacja zadań wynikających z kodeksu ISPS możliwa jest tylko wówczas, gdy pracownicy posiadają rzetelną wiedzę i umiejętności oraz świadomość zagrożeń. Cała organizacja musi charakteryzować się wysoką kulturą bezpieczeństwa.

Kultura bezpieczeństwa szczególnie w przedsiębiorstwie ochrony musi być oparta na trzech filarach [16]:

- sferze kultury mentalnej – związanej m.in. z poziomem wiedzy o bezpieczeństwie;
- sferze kultury materialnej – m.in. technice i technologii, infrastrukturze, sprzęcie;
- sferze kultury organizacyjnej – obejmującej m.in. regulacje prawne, strukturę organizacyjną oraz sposoby i procedury działania.

Sfera kultury organizacyjnej jest coraz silniej związana z wykorzystaniem nowoczesnych technologii informacyjno-komunikacyjnych, które zaczynają stanowić trzon technicznych systemów ochrony. Właściwe kształtowanie środowiska bezpieczeństwa w wymiarze personalnym, instytucjonalnym i technicznym jest ważnym elementem systemów zarządzania kryzysowego w portach morskich.

Literatura

1. Tubielewicz A.: Zarządzanie strategiczne w portach morskich: globalizacja, integracja, prognozowanie, planowanie, strategie. PAN, Gdańsk, 2004.
2. Forkiewicz M., Tubielewicz A.: Management of seaport critical infrastructures of integrated sea-land transport chains. (w:) Fertsch M., Stachowiak A. (eds.): Problems of transport logistics. Poznań University of Technology, Poznań 2010, s. 111–128.
3. Tubielewicz A., Forkiewicz M., Kowalczyk P.: Zarządzanie kryzysowe w portach morskich. Knosala R. (red.): Komputerowo zintegrowane zarządzanie. T. 2 Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Opole 2010, s. 580–586.

4. Międzynarodowy kodeks ochrony statku i obiektu portowego – Kodeks ISPS, 2002 r.
5. Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów. Dz.U. UE, L. 310, z dnia 25 listopada 2005.
6. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony. Dz.U. UE, L. 345, z dnia 23 grudnia 2008.
7. Ustawa z dnia 4 sierpnia 2008 r. o ochronie żeglugi i portów morskich, Dz.U. nr 171, poz. 1055 z 2008 r. z późn. zm.
8. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. nr 89, poz. 590 z 2007 r. i Dz.U. nr 131, poz. 1076 z 2009 r. z późn. zm.
9. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Dz.U. nr 114, poz. 740 z 1997 r. z późn. zm.
10. Ustawa z dnia 21 maja 1999 r. o broni i amunicji, Dz.U. nr 52, poz. 525 z 2004 r. z późn. zm.
11. Misiuk A.: Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe. Wydawnictwa Akademickie i Profesjonalne. Warszawa 2008.
12. Tubielewicz A., Forkiewicz M., Kowalczyk P.: Assessment of port facilities security in crisis management. Polish Journal of Environmental Studies, vol. 19, no 4A, 2010, s. 111–114.
13. Tubielewicz A., Forkiewicz M., Kowalczyk P.: Planning of the seaports critical infrastructure protection in the light of the ISPS Code requirements. Scientific Journals, Maritime University of Szczecin, vol. 24(96), 2010, s. 35–140.
14. Blim M.: Bezpieczeństwem fizyczne. Ochrona obiektu i wartości. (w:) Staniec I., Zawiła-Niedźwiecki J.: Zarządzanie ryzykiem operacyjnym. C.H. Beck, Warszawa 2008, s. 229–260.
15. Szustakowski M., Ciurapiński W.: Projektowanie systemów ochrony technicznej mienia, obiektów i obszarów. VI Międzynarodowa Konferencja Naukowa Zarządzanie Kryzysowe, Olsztyn, 19–21 czerwca 2008, www.uwm.edu.pl/mkzk.
16. Cieślarczyk M.: Kultura bezpieczeństwa w sytuacjach kryzysowych. (w:) Jabłonowski M., Smolak L. (red. nauk.): Zarządzanie kryzysowe w Polsce. Pułtusk 2007, s. 349–370.

Praca naukowa finansowana ze środków na naukę w latach 2009–2011 jako projekt rozwojowy: „Model zarządzania kryzysowego bezpieczeństwem na obszarach portów morskich”.

Dr inż. Marcin FORKIEWICZ
Katedra Zarządzania
Wydział Zarządzania i Ekonomii
Politechnika Gdańska
80–233 Gdańsk, ul. Narutowicza 11/12
tel./fax: (0-58) 347 24 55 / (0-58) 348 60 24
e-mail: mfork@zie.pg.gda.pl