

# Zintegrowany system **ochrony** lotniska



FOT. ANNA TARACZUK

Leszek Loroeh, Przemysław Mądrzycki, Monika Świech

**« SKUTECZNA OCHRONA INFRASTRUKTURY KRYTYCZNEJ STAŁA SIĘ W XXI WIEKU JEDNYM Z GŁÓWNYCH WYZWAŃ DLA BEZPIECZEŃSTWA. INFRASTRUKTURA KRYTYCZNA JEST SZCZEGÓLNIENIE NARAŻONA NA ATAK TERRORYSTYCZNY, A JEJ ZNISZCZENIE CZY NAWET TYLKO USZKODZENIE NIESIE ZE SOBĄ POWAŻNE KONSEKWENCJE NIE TYLKO DLA ZABEZPIECZENIA OD ATAKU (SECURITY), ALE RÓWNIEŻ DLA BEZPIECZEŃSTWA (SAFETY) ROZUMIANEGO JAKO NORMALNE FUNKCJONOWANIE.**

Celami ataków terrorystycznych w Europie Zachodniej oraz Stanach Zjednoczonych są przede wszystkim cywilne obiekty o znaczeniu strategicznym, takie jak sieci transportowe i telekomunikacyjne, centra finansowe i budynki administracji publicznej.

Konsekwencją nasilenia się działań terrorystycznych stała się tak zwana wojna z terroryzmem. Doświadczenia pokazały, że lotniska są częstym obiektem ataków, a odpowiednie ich zabezpieczenie ma w tej sytuacji ogromne znaczenie.

Postęp technologiczny umożliwia skuteczną ochronę infrastruktury krytycznej za pomocą coraz bardziej zaawansowanych i czułych sensorów różnych typów. Wraz z rozwojem samych sensorów, następuje integracja systemów oraz rozwój systemów transmisji danych. Wiodącą rolę odgrywają tu techniki telekomunikacyjne i satelitarne. Jednak rozwój technologii z jednej strony usprawnia obronę przed zagrożeniami, ale z drugiej może być wykorzystany do coraz bardziej skutecznego ataku na infrastrukturę krytyczną. Z tego względu istotne jest systemowe podejście do zagadnienia ochrony infrastruktury krytycznej, gdyż tylko takie może zapewnić kompleksowy nadzór nad danym obszarem. W wypadku, gdy informacja pozyskiwana jest z różnych źródeł (sensorów) tworzących system, podstawowym problemem staje się zagadnienie obróbki oraz fuzji danych. Umiejętność przetworzenia danych i przedstawienia ich w określonym formacie, niezależnie od rodzaju użytych interfejsów, pozwala na integrację systemów (*system of systems*).

Kluczowe technologie dla systemów bezpieczeństwa mieszczą się w priorytetach programów ramowych Unii Europejskiej, a także w priorytetach technologicznych Europej-

skiej Agencji Obrony. Wykorzystanie nowoczesnych technologii umożliwić powinno poprawienie poziomu wiedzy o zagrożeniach (*situational awareness*), ochronę przed użyciem substancji biologicznych, chemicznych, radioaktywnych oraz wysokoenergetycznych, usprawnienie procesów zarządzania kryzysowego oraz interoperacyjność i integrację systemów informacyjnych i łączności.

W niniejszym artykule przedstawiono czynniki mające wpływ na kształt projektowanego systemu monitorowania zagrożeń, w tym w szczególności zagrożeń zewnętrznych, oraz sensory lub komponenty, które mogą zostać w nim wykorzystane.

## « LOTNISKO JAKO OBIEKT OCHRONY

Lotnisko jest obiektem trudnym do ochrony i monitorowania. Czynniki wpływające na taki stan są następujące jego cechy:

■ **Złożoność, rozległość i zróżnicowanie pod względem występującej infrastruktury.**

Lotnisko najczęściej jest zlokalizowane na dużym obszarze, często graniczącym z naturalnymi kompleksami leśnymi. Taka lokalizacja wymaga stosowania ogrodzeń oraz fizycznych przeszkód trudnych do monitorowania tradycyjnymi metodami. Konwencjonalne zabezpieczenia (plot, szlabany, punkty kontrolne) nie stanowią dostatecznej przeszkody dla wtargnięcia do wewnętrznej strefy lotniska.

■ **Kłopotliwość pod względem ochrony strefy zewnętrznej i obiektów wewnętrznych.**

Ochrona tak rozległego obiektu jest kłopotliwa i kosztowna. Ochrona metodami konwencjonalnymi z wykorzystaniem przeszkód fizycznych najczęściej nie daje możliwości alarmowania o wtargnięciu na teren bazy lub czas reakcji uniemożliwia podjęcie przeciwdziałania. Tym samym pomimo dobrych zabezpieczeń strefy zewnętrznej możliwe jest wtargnięcie intruza do strefy wewnętrznej.



### ■ Kumulacja „punktów wrażliwych”

Na terenie lotniska zlokalizowane są obiekty i systemy mające kluczowe znaczenie dla możliwości operacyjnego wykorzystania stajonujących tam statków powietrznych. Są to składy paliwa, systemy informatyczne, zasilania, tankowania itp. Tym samym zagrożeniem dla prawidłowego funkcjonowania lotniska może być uszkodzenie lub zniszczenie wybranego „punktu wrażliwego”.

### ■ Trwała uszkodzalność

Na lotniskach wykorzystywane są specyficzne systemy i urządzenia. Najczęściej nie można w krótkim czasie zastąpić uszkodzonego lub zniszczonego urządzenia innym. Tym samym zniszczenia lub uszkodzenia specyficznych urządzeń lub systemów mogą mieć charakter trwały, eliminujący całe lotnisko z operacyjnego wykorzystania.

### ■ Powtarzalna struktura obiektów

Lotniska różnią się pomiędzy sobą szczególnie wielkością. Mają jednak zbliżoną infrastrukturę charakterystyczną dla lotnisk komunikacyjnych. Znajomość tej infrastruktury oraz zasad jej operacyjnego wykorzystania jest czynnikiem ułatwiającym działanie potencjalnego agresora.

### ■ Medialność lotniska

Jednym z aspektów działania terrorystycznego jest uzyskanie jak największego rozgłosu medialnego. Atak na lotnisko zapewnia odpowiednie „nagłośnienie” ataku oraz natychmiastową reakcję mediów.

Biorąc pod uwagę powyższe cechy charakterystyczne lotnisk można wyodrębnić następujące strefy ochrony:

**Strefa I** – pas terenu od ogrodzenia lotniska do 300 – 500 m na zewnątrz oraz przedłużenia pasów startowych o 3 – 5 km.

**Strefa II** – ogrodzenie lotniska.

**Strefa III** – teren od ogrodzenia lotniska do zabudowań wewnętrznej infrastruktury.

**Strefa IV** – zabudowania lotniska.

**Strefa V** – ochrona wnętrza budynków.

**Strefa 0** – obiekty o specjalnym znaczeniu („punkty wrażliwe – wieża kontroli lotów, hala przylotów i odlotów”).

Ochrona tak dużego obszaru, bardzo zróżnicowanego pod względem możliwości stosowania środków i urządzeń ochrony, stanowi ogromne techniczne i organizacyjne wyzwanie. Monitorowanie zewnętrznego zagrożenia lotniska prowadzić można, wykorzystując zarówno stałe elementy obserwacyjne, jak i elementy mobilne; zawierające czujniki (sensory) radarowe, optyczne, zagrożeń biologicznych, chemicznych i ra-

Jednym z aspektów działania terrorystycznego jest uzyskanie jak największego rozgłosu medialnego. Atak na lotnisko zapewnia odpowiednie „nagłośnienie” ataku oraz natychmiastową reakcję mediów.

diologicznych. Dlatego prace koncepcyjne i konstrukcyjne systemu ochrony powinny uwzględniać efekt „nadmiaru informacji” oraz efektywne wykorzystywanie poszczególnych komponentów.

### « MOŻLIWY SKŁAD SYSTEMU

Ze względu na złożoność planowanego systemu należy przewidzieć zastosowanie całej gamy różnych środków ochrony, dostosowanych do lokalnych potrzeb. Należy się również liczyć z koniecznością stworzenia lokalnych ośrodków ochrony oraz centralnego centrum ochrony. Struktura taka wynika z możliwości pojawienia się problemu „nadmiaru informacji” w wypadku integracji systemu z wykorzystaniem jednego – centralnego centrum ochrony. Przyjmuje się, że w skład zintegrowanego systemu powinny wchodzić następujące komponenty:

#### Środki ochrony fizycznej:

- szlabany,
- bariery,
- zapory.

#### Środki monitoringu wejścia – wyjścia:

- systemy detekcji metalu, broni, środków wybuchowych itp.

#### Kamery z systemem rejestracji:

- systemy identyfikacji (w tym sensory biometryczne)

#### Detektory i systemy:

- detektory pasywne,
- systemy obserwacyjne TV/IR,
- masztowe systemy obserwacyjne,
- radiolokacyjne systemy wykrywania,
- radiolokacyjne systemy obserwacyjne,
- systemy kontroli dostępu.

#### Infrastruktura informatyczna

#### Systemy łączności i transmisji danych i obrazu

#### Elementy integracyjne

#### Lokalne ośrodki ochrony

#### Główne centrum ochrony

Elementy tworzące zintegrowany system ochrony powinny zostać zintegrowane w sposób zapewniający uzyskanie wspólnej przestrzeni informacyjnej umożliwiającej nadzór nad ochranianym obszarem.



### AGENCJA NA LOTNISKU

Niewykluczone, że Agencja Mienia Wojskowego stanie się współwłaścicielem Portu Lotniczego Poznań Ławica. Wszystko z powodu braku gruntów koniecznych do dalszej rozbudowy lotniska. Potrzebnym terenem, na którym mieszczą się obiekty powojenne, dysponuje Agencja Mienia Wojskowego. Lotnisko dzierżawi znajdujące się tam hangary. Fort chciałby przejąć te tereny i розміścić na nich port towarowy – cargo. AMW jest z kolei zainteresowana wnieśieniem terenów aportem do spółki, podwyższeniem jej kapitału i staniem się jednocześnie nowym udziałowcem portu. Obecni właściciele, Przedsiębiorstwo Państwowe Porty Lotnicze (62,5 proc.), miasto Poznań (25 proc.) i województwo wielkopolskie (12,5 proc.) nie wykluczają takiej możliwości.

### SUSŁY LOTNISKOWE

Władze województwa lubelskiego chcą portu lotniczego w Świdniku. Tym samym zrezygnowano z dotychczasowej lokalizacji w Niedźwiedzie, którą uznano za nieekonomiczną. – Budowa portu lotniczego w Niedźwiedzie kosztowałaby miliard złotych. Przy założeniu, że Unia Europejska sfinansowałaby połowę tej kwoty, województwo musiałoby wyłożyć 500 milionów. Na tyle nas nie stać – mówi Jarosław Zdrojowski, marszałek województwa. – Poza tym w Niedźwiedzie nie ma niezbędnej infrastruktury. Trzeba by tam doprowadzić energię elektryczną, sieć wodno-kanalizacyjną, wybudować drogi i linię kolejową, co oznaczałoby następne koszty. Dlatego zdecydowaliśmy się na przeniesienie lotniska w Świdnik. Problemem mogą się jednak okazać... sąsiedzi pensjonariusze, które założyły swoją kolonię w okolicach terenów przeznaczonych pod inwestycję. Ekolodzy już zapowiedzieli protesty. Krzysztof Gorczyca, prezes Towarzystwa dla Natury i Człowieka w Lublinie, nie zgadza się na przeniesienie kolonii sasków w inne miejsce. – Były w przeszłości próby przenoszenia kolonii sasków w inne miejsce, ale to nic nie dało. Zwierzątka żyły w nowych miejscach najwyżej dwa lata i cała kolonia zniknęła. „Susły albo lotnisko” zatytułował swój artykuł „Kurier Lubelski”.

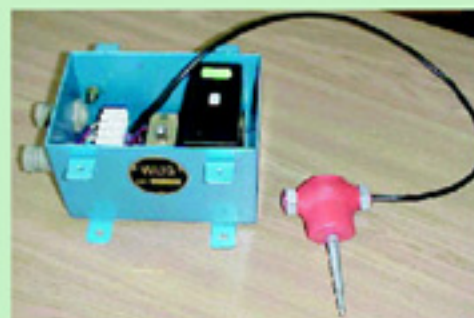




## OPIS WYBRANYCH DETEKTORÓW

### « PASYWNY DETEKTOR SEJSMICZNY

Detektor wykrywa odgłosy kroków lub pojazdu poruszającego się w otoczeniu miejsca zainstalowania czujnika. Jest wyposażony w nadajnik radiowy wysyłający sygnał o zadziałaniu do lokalnego lub głównego centrum ochrony. Czułość detektora może być dostosowana do aktualnego poziomu nagłośnienia na ochranianym terenie.



Fot. 1. Pasywny detektor sejsmiczny

Sposób zainstalowania wyklucza wykrycie go przez agresora. Detektory są tanie i niezawodne. Łatwe w integrowaniu z innymi komponentami. Sieć takich czujników może stanowić pierwszą linię ochrony strefy zewnętrznej. Zadziałanie czujnika może w sposób skryty aktywizować inne systemy, np. masztowy system obserwacyjny. Czujnik może być wykorzystywany w strefach I, II, III oraz O.

### « MASZTOWY SYSTEM OBSERWACYJNY

Masztowe systemy obserwacyjne często stanowią integralny środek ochrony i obserwacji w warunkach dziennych i nocnych.

W ich skład najczęściej wchodzi:

- maszt stały lub mobilny,
- głowica obserwacyjna TV/IR,
- stanowisko operatora, pełniące często funkcję lokalnego ośrodka przetwarzania i przesyłania danych.

Systemy takie mogą być wykorzystywane do stałej ochrony lotniska lub jako system mobilny do ochrony wskazanego obiektu lub obszaru. Na szczycie masztu umieszcza się głowice obserwacyjne pracujące w pasmach promieniowania widzialnego i termalnego. Ponadto można zastosować radiolokacyjny system obserwacyjny. Taka konfiguracja sensorów zapewnia wykrywanie pojedynczej osoby w promieniu od 6 km do 10 km wokół masztu, niezależnie od

Fot. 2. Maszt w stanie złożonym



Fot. 3. Masztowy system w stanie rozłożonym

pory dnia czy nocy oraz w złych warunkach pogodowych. W zależności od potrzeb obraz z sensorów może być przesyłany do lokalnego centrum ochrony, zabudowanego w kontenerze lub do głównego centrum ochrony z wykorzystaniem systemu transmisji.

Masztowy system obserwacyjny ze względu na zasięg obserwacji może być wykorzystywany do ochrony w strefach I, II, III i IV.

### « RADIOLOKACYJNE SYSTEMY OBSERWACYJNE

Radiolokacyjne systemy obserwacji mogą być stosowane jako komponenty działające samodzielnie lub zintegrowane z innymi

systemami lub detektorami. Mogą być montowane na ochranianych obiektach, ogrodzeniach lub w systemie masztowym. Zapewniają wykrycie i śledzenie poruszających się obiektów niezależnie od warunków pogodowych dnia czy nocy. Mogą być wykorzystywane do ochrony w strefach: I, II, III i O.



Fot. 4. Radiolokacyjny system obserwacji

### « SYSTEMY OBSERWACYJNE TV/IR

Systemy obserwacji TV/IR mogą być wykorzystywane w wielu wariantach zastosowania w systemie. Mogą pracować samodzielnie lub tworzyć „sieć” sensorów. Zapewniają wykrycie obiektu wielkości człowieka z odległości ok. 1 km w warunkach dziennych i nocnych oraz w złych warunkach pogodowych. Mogą być wyposażone w system automatycznego ostrzegania o wystąpieniu zagrożenia. W zależności od potrzeb mogą realizować funkcję samodzielnego przeszukiwania terenu w zadeklarowanych przez użytkownika kierunkach. Ze względu na swoje walory użytkowe znajdują zastosowanie we wszystkich strefach ochronnych bazy.





Fot. 5. System obserwacji TV/IR

## « ZASADY INTEGRACJI

Podstawową zasadą integracji poszczególnych komponentów musi być uzyskanie przestrzeni informacyjnej pozwalającej monitorować ochraniający obszar bez efektu „nadmiaru informacji”. Zgromadzenie i wizualizacja w jednym miejscu dużej liczby sygnałów i obrazów z systemów obserwacyjnych spowoduje utratę możliwości efektywnego ochrania. Doświadczenia z wdrożenia systemu obserwacyjnego wskazują, iż po 2 godzinach prowadzenia obserwacji zmęczenie operatora jest tak duże, iż łatwo może popełnić błąd. Dlatego integrację powinna charakteryzować hierarchiczność sensorów. Detektory pasywne powinny aktywizować systemy złożone, np. obserwacyjne. Kolejną zasadą, która powinna być uwzględniona w procesie integracji jest tworzenie lokalnego ośrodka ochrony. W celu uniknięcia nadmiaru informacji – do ośrodka centralnego powinna napływać tylko informacja niezbędna. W wypadku systemu złożonego i rozbudowanego, ośrodek centralny powinien być alarmowany dopiero po zaistnieniu zagrożenia. Uzyskane informacje powinny być weryfikowalne. Dlatego należy zakładać redundancję stosowanych detektorów. Idealem byłaby możliwość potwierdzenia wystąpienia zagrożenia przez inny detektor lub system.

Integracja powinna przewidywać możliwość rozbudowy o kolejne elementy pasywne lub aktywne. Wiąże się to z koniecznością zastosowania architektury otwartej.

Oprócz systemów i detektorów wykrywających zagrożenie lub monitorujących obszar, niezbędne jest również zintegrowanie w jeden funkcjonalny system lub podsystem środków łączności i transmisji obrazu.

**Zintegrowany system będzie skuteczny na tyle, na ile efektywny będzie jego najdrobniejszy element (detektor). Decyzja o budowie systemu zintegrowanego implikuje zastosowanie elementów i komponentów o określonym poziomie technologicznym.**

## « PODSUMOWANIE

■ Bezpieczeństwo lotnisk w świetle działań terrorystycznych stanowi niezwykle istotny problem, związany z bezpieczeństwem każdego kraju.

■ Każdy z ochraniających obiektów jest inny, ma swoją specyfikę oraz określone ograniczenia w stosowaniu środków ochrony. Tworzenie systemu zintegrowanego musi być poprzedzone szczegółową analizą zarówno możliwości technicznych, jak i możliwych zagrożeń.

■ Zintegrowany system będzie skuteczny na tyle, na ile efektywny będzie jego najdrobniejszy element (detektor). Decyzja o budowie systemu zintegrowanego implikuje zastosowanie elementów i komponentów o określonym poziomie technologicznym.

■ Żaden z opracowanych systemów ochrony nie jest doskonały. W miarę upływu czasu staje się coraz bardziej „otwarty” i łatwiejszy do pokonania. Dlatego funkcjonowanie systemu musi być wsparte odpowiednimi procedurami codziennych zachowań wszystkich osób pracujących na chronionym terenie. «

## Z KATOWIC DO USA

„Katowickie Pyrzowice starają się o otwarcie bezpośredniego połączenia ze Stanami Zjednoczonymi. Rozmowy w tej sprawie są prowadzone z PLL LOT i irlandzkim Ryanair. Zarząd województwa śląskiego złożył ponadto firmie Ryanair ofertę założenia na lotnisku w Pyrzowicach bazy obsługującej loty do Stanów Zjednoczonych. Negocjacje w tej kwestii trwają również z LOT-em. Według Michaela O’Leary’ego, szefa Ryanaira, jego firma może zacząć latać nad Atlantyką dopiero w 2009-2010 roku. Tyle czasu potrzebuje na kupno odpowiednich samolotów. Nie jest również wykluczone, że do obsługi lotów transatlantyckich O’Leary stworzy nową spółkę, niezwiązaną z Ryanaiem.

## BĘDĄ OBICE?

Przemysław Gosiewski, znany polityk PiS forsuje kontrowersyjny plan budowy międzynarodowego lotniska w Obicach pod Kielcami, na które chciałby przeznaczyć 300 mln zł z publicznej kasy. Według „Gazety Wyborczej”, żeby utrzymać lotnisko, potrzeba rocznie minimum 200 tys. podróży. Tymczasem prezydent Kielc wyliczył, iż za osiem lat w Obicach może ich być 150 tysięcy. Przez pierwsze kilka lat Obice na pewno będą przynosić straty – konkluduje gazeta. Na razie postanowiono, że koncepcję budowy podkieleckiego lotniska przygotowuje londyńska firma Ove Arup & Partners International Ltd. Brytyjczycy zajmą się także studium wykonalności, analizą kosztów oraz raportem oddziaływania inwestycji na środowisko. Ministerstwo Transportu rozpoczęło wdrażanie programu wykorzystania środków funduszy europejskich przeznaczonych na rozwój infrastruktury lotniczej. W latach 2007 – 2013 największe porty lotnicze w kraju (Warszawa, Kraków, Katowice, Gdańsk, Wrocław, Poznań, Szczecin i Rzeszów) otrzymają wsparcie w wysokości 350 milionów euro. Pozostałe lotniska mogą sięgać po środki z funduszy regionalnych, a także w ramach programu „Bezpieczeństwo transportu i krajowe sieci transportowe”, gdzie na projekty związane z bezpieczeństwem transportu lotniczego we wszystkich portach obsługujących ruch międzynarodowy zarezerwowano kwotę ok. 50 mln euro.

## SAMORZĄD CHCE LOTNISKA

Samorząd województwa mazowieckiego chce stać się udziałowcem spółki Port Lotniczy Radom SA. Sejmik wojewódzki popiera budowę portu lotniczego w Radomiu, która została wpisana do listy projektów finansowanych z funduszy strukturalnych Unii Europejskiej. Na utworzenie lotniska cywilnego w Radomiu mają być przeznaczone 32 mln zł. Na razie władze miasta przejęły 3 ha terenu od Agencji Mienia Wojskowego. Jednak jest to za mało na potrzeby lotniska. Realizacja inwestycji jest uzależniona od pozyskania kolejnych 20 ha od wojska, jednak nie wiadomo, na jakich zasadach mogłyby one być przekazane spółce. Spółka ma już zgodę na zarządzanie portem lotniczym, wydaną przez ministra transportu i ministra obrony narodowej.

LITERATURA: [1] Sprawozdanie z prezentacji Systemu Obserwacji Terenu. Instytut Techniczny Wojsk Lotniczych, WARSZAWA 2004, Nr BT ITWL 1893/5. [2] Mądrycki P, Szczepański C, Karcznarz D, Puchalski W, Butlewski K, Marchwicki R: Integracja i badania systemu obserwacji terenu. Instytut Techniczny Wojsk Lotniczych, WARSZAWA 2004, Nr BT ITWL 1897/5. [3] System ochrony bazy. Instytut Techniczny Wojsk Lotniczych, WARSZAWA 18.05.2005, Materiały z seminarium. [4] Sprawozdanie z prac wdrożeniowych Stacjonarnego Systemu Obserwacji Terenu w Bazie ECHO Diwanah. Instytut Techniczny Wojsk Lotniczych, 2006.