Problematyka niezawodnościowo-eksploatacyjna systemów ochrony peryferyjnej portów lotniczych

Mirosław Siergiejczyk, Adam Rosiński, Karolina Krzykowska

Port lotniczy jest obiektem, który umożliwia spełnienie wszystkich oczekiwań i osiągnięcie celów terroryzmu: duże skupiska osób, niekontrolowany dostęp do stref ogólnodostępnych oraz ogromne zniszczenia w przypadku przeprowadzonego zamachu. Dlatego też bardzo istotne jest stosowanie najnowocześniejszych systemów bezpieczeństwa. W artykule zaprezentowano przykładowe rozwiązania z zakresu ochrony peryferyjnej obiektów o znaczeniu strategicznym. Dokonano także analizy niezawodnościowo-eksploatacyjnej zintegrowanego systemu ochrony peryferyjnej portu lotniczego. Uzyskane zależności pozwalają obliczyć wartości prawdopodobieństw przebywania systemu w wyróżnionych stanach. Stosując je, można porównać różnego rodzaju rozwiązania i dokonać wyboru optymalnego przy założonych kryteriach wstępnych.

Prof. nzw. dr hab. inż. Mirosław Siergiejczyk
Zakład Telekomunikacji w Transporcie
Wydział Transportu
Politechnika Warszawska
00-662 Warszawa, ul. Koszykowa 75
msi@wt.pw.edu.pl

Dr inż. Adam Rosiński
Zakład Eksploatacji Systemów Elektronicznych
Instytut Systemów Elektronicznych, Wydział Elektroniki, Wojskowa Akademia Techniczna
00-908 Warszawa
ul. gen. S. Kaliskiego 2
arosinski@wat.edu.pl

Mgr inż.
Karolina Krzykowska
Zakład Telekomunikacji w Transporcie
Wydział Transportu
Politechnika Warszawska
00-662 Warszawa, ul. Koszykowa 75
kkrzykowska@wt.pw.edu.pl

Wstęp

W dokumencie „Narodowy Program Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej zdefiniowano 11 systemów, które wchodzą w skład infrastruktury krytycznej. Mają one kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli. Zapewniają także prawidłowe funkcjonowanie organów administracji publicznej, instytucji rządowych i przedsiębiorców. W skład infrastruktury krytycznej zaliczane są następujące systemy [9]:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągi substancji niebezpiecznych).

Spośród wymienionych systemów bardzo ważnym jest transport. Jest to przemieszczanie ludzi, ładunków (przedmiot transportu) w przestrzeni przy wykorzystaniu odpowiednich środków transportu. Przemieszczanie dóbr, ludzi i usług jest jedną z podstawowych cech charakteryzujących współczesną gospodarkę i społeczeństwo. Dlatego też sprawnie funkcjonujący system transportowy stanowi jeden z filarów nowoczesnego państwa. Zatem istotne jest zapewnienie bezpieczeństwa obiektom (zarówno stacjonarnym jak i ruchomym) wykorzystywanym w procesie transportowym [2,3]. W tym celu wykorzystuje się różne rozwiązania.

System pełnej sygnalizacji zagrożeń (tzw. ochrony elektronicznej) tworzy się z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń, jako systemy [15]:

- sygnalizacji włamania i napadu [6],
- sygnalizacji pożaru,
- kontroli dostępu,
- monitoringu wizyjnego [5],
- ochrony terenów zewnętrznych.

Ochrona wynikająca z działania tych systemów może być uzupełniona przez systemy:

- sygnalizacji stanu zdrowia lub zagrożenia osobistego,
- sygnalizacji zagrożeń środowiska,
- przeciwkradzieżowe,
- dźwiękowe systemy ostrzegawcze,
- zabezpieczenia samochodów przed włamaniem i uprowadzeniem.

Najkorzystniej (z punktu widzenia zapewnienia poziomu bezpieczeństwa) jest zastosować elektroniczne systemy bezpieczeństwa i odpowiednie służby ochrony, które powiązane są między sobą poprzez odpowiednie procedury działania. W artykule ukazano wykorzystanie różnych systemów ochrony peryferyjnej do ochrony obiektów. Dokonano także analizy niezawodnościowo-eksploatacyjnej systemów ochrony peryferyjnej, które są stosowane m.in. w portach lotniczych.

Port lotniczy jest miejscem przeznaczonym do użytku publicznego. Jego głównym zadaniem jest zapewnienie odpowiednich i bezpiecznych warunków do obsługi pasażerów i towarów odbywających podróże wykorzystując statki powietrzne. Możliwe jest to m.in. poprzez współpracę instytucji państwowych i pozapaństwowych w zakresie bezpieczeństwa. Powinny one zapewnić odpowiedni poziom bezpieczeństwa następującym obiektom [1]:

- terminale pasażerskie oraz inne terminale,
- wieża kontroli ruchu lotniczego,
- generatory energetyczne,
- magazyny paliw i smarów,
- systemy klimatyzacyjne i wentylacyjne,
- bocznice kolejowe,
- ujęcia wody,
- płyty postojowe statków powietrznych,
- hangary,
- inne urządzenia bądź obiekty uznane przez Prezesa Urzędu Lotnictwa Cywilnego (ULC) lub zarządzającego lotniskiem za istotne dla ochrony lotnictwa cywilnego (np. urządzenia systemów wspomagania lądowania).

Obiekty znajdujące się w obszarze portu lotniczego chroni się ze względu na zagrożenia naturalne oraz te wywoływane przez człowieka. Jako zagrożenia naturalne uważa się wszelkie anomalie pogodowe i czynniki naturalne, które uniemożliwiają normalną eksploatację portu lotniczego. Na nie służby mające zapewnić bezpieczeństwo mają stosunkowo mały wpływ. W większym zakresie mogą za to wpływać na niebezpieczeństwa, które są spowodowane przez człowieka.

Można wymienić kilka przykładowych i najbardziej istotnych zagrożeń:

- bezprawne wniesienie do strefy zastrzeżonej przedmiotów niedozwolonych ujętych w rozporządzaniu komisji (UE) nr 185/210 [7],
- bezprawne wtargnięcie do strefy zastrzeżonej,
- zagrożenie podłożenia lub podłożenie materiałów wybuchowych w obiektach portu lotniczego,
- zagrożenie użycia bądź użycie bioterroryzmu (broń biologiczna),
- atak z użyciem broni na osoby przebywające w obszarze portu lotniczego,
- wniesienie na pokład statku powietrznego materiałów wybuchowych bądź przedmiotów niedozwolonych do przewozu transportem lotniczym,
- wzięcie zakładników na terenie portu lotniczego,
- zawładnięcie statkiem powietrznym (z pasażerami lub bez),
- prowadzenie aktów sabotażu, dywersji, wandalizmu lub o jakimkolwiek charakterze kryminalnym,
- lądowanie w porcie lotniczym statku powietrznego z terrorystami na pokładzie,
- wszelkie zakłócenia porządku publicznego, np. poprzez demonstracje lub inne formy protestu.

Wobec tak licznych i różnorodnych niebezpieczeństw [4] istotne jest, by zintegrowany system bezpieczeństwa możliwie jak najszerzej im przeciwdziałał [8]. Dlatego też stosuje się systemy ochrony peryferyjnej, w skład których wchodzą różnego rodzaju podsystemy. Zachowanie ich w stanie zdatności jest zatem niezbędne, by prawidłowo realizowały funkcje do których zostały zaprojektowane. W dalszej części artykułu zostanie przeprowadzona analiza niezawodnościowo-eksploatacyjna zintegrowanego systemu ochrony peryferyjnej.

Ochrona peryferyjna portu lotniczego

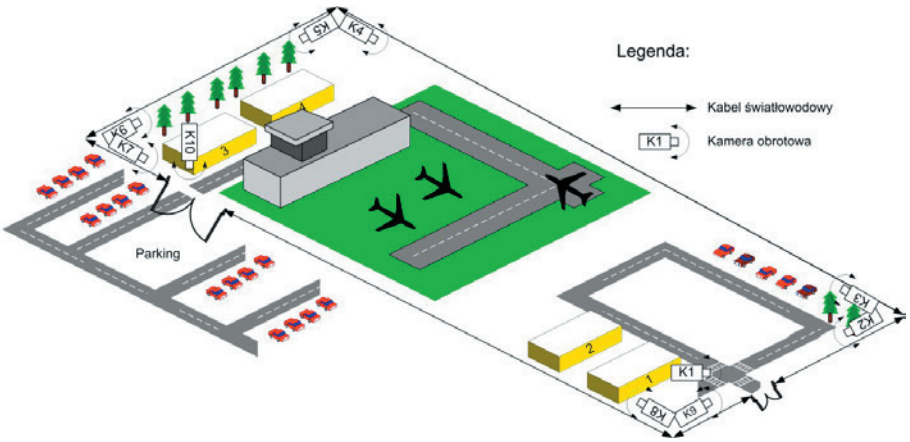
W porcie lotniczym należy jak najszybciej wykryć zagrożenie, ponieważ umożliwi to podjęcie racjonalnych działań. Dlatego też tak istotne jest miejsce wykrycia osoby nieuprawnionej. W ten sposób można zminimalizować ewentualne straty w przypadku wystąpienia zagrożenia dla portu lotniczego. W tym celu opracowano wiele metod ochrony peryferyjnej obiektów o specjalnym znaczeniu, które to wykorzystują różne prawa i właściwości zjawisk fizycznych. Wybór określonego rozwiązania zależy m.in. od:

- czynników środowiskowych (czynniki atmosferyczne w tym nasłonecznienie, opady deszczu i śniegu, mgła; zakłócenia elektromagnetyczne),
- warunków instalacyjnych (miejsce montażu urządzeń, wytyczne zawarte w dokumentacji producenta, zapewnienie dostępu służb serwisowych),
- wymagań zawartych w obowiązujących aktach prawnych i innych rozporządzeniach i wytycznych w zakresie ochrony danego obszaru,
- innych wymagań inwestora i użytkownika (np. koszty urządzeń i ich instalacji, a także późniejszej eksploatacji, wewnętrznych procedur w ochranianym obiekcie).

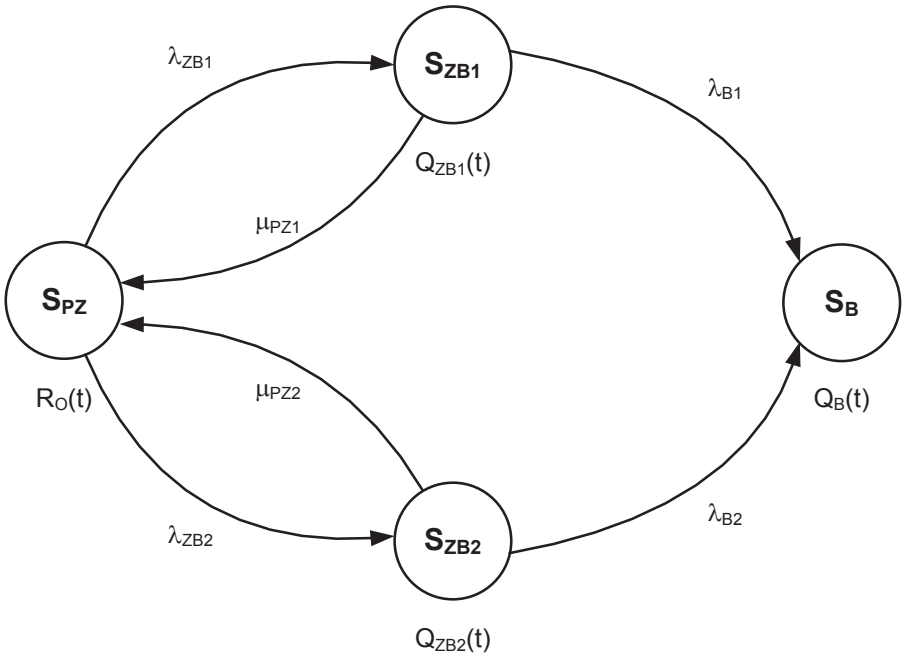
Współczesne systemy ochrony peryferyjnej obiektów o specjalnym przeznaczeniu (w tym portów lotniczych) można podzielić na:

- systemy ogrodzeniowe instalowane na wewnętrznym ogrodzeniu obwodnicy,
- naziemne systemy ochrony zewnętrznej,
- ziemne systemy ochrony zewnętrznej.

Do ziemnych systemów ochrony zewnętrznej można zaliczyć m.in. kabel światłowodowy. Zazwyczaj jest on znany jako medium transmisyjne wykorzystywane do budowy sieci telekomunikacyjnych. Jednakże ze względu na swoje właściwości, może też być wykorzystany jako element detekcyjny systemu ochrony peryferyjnej. Wykrywa on wówczas nacisk lub wibracje, które są powodowane przez osobę nieuprawnioną do przekroczenia granicy obszaru zastrzeżonego. Cechy światłowodu powodują, że to roz-



***1**. Widok portu lotniczego z zastosowanymi systemami bezpieczeństwa*



***2**. Relacje w zintegrowanym systemie ochrony peryferyjnej portu lotniczego*

Oznaczenia na rys.:

$R_O(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie pełnej zdatności,
$Q_{ZB}(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zagrożenia bezpieczeństwa,
$Q_B(t)$ – funkcja prawdopodobieństwa przebywania systemu w stanie zawodności bezpieczeństwa,
λ_{ZB1}, λ_{ZB2} – intensywności przejść ze stanu pełnej zdatności do stanu zagrożenia bezpieczeństwa,
μ_{PZ1}, μ_{PZ2} – intensywności przejść ze stanu zagrożenia bezpieczeństwa do stanu pełnej zdatności,
λ_{B1}, λ_{B2} – intensywności przejść ze stanu zagrożenia bezpieczeństwa do stanu zawodności bezpieczeństwa.

wiązanie jest całkowicie odporne na zakłócenia elektromagnetyczne. Dzięki temu, że nie przewodzi elektrycznego sygnału, można go bezpiecznie stosować w pobliżu linii energetycznych, systemów radarowych. Jest to szczególnie istotne w zastosowaniu tego rozwiązania w porcie lotniczym i innych obiektach gdzie występują stacje radiolokacyjne [13]. Zaletą jest też odporność chemiczna, która pozwala na zastosowanie w środowisku agresywnym chemicznie. Do wad należy zaliczyć: koszt instalacji związany z pracami ziemnymi, koszt urządzeń oraz koszt naprawy ewentualnych uszkodzeń kabla.

Do naziemnych systemów ochrony zewnętrznej można zaliczyć m.in. systemy monitoringu wizyjnego (ang. CCTV – Closed Circuit TeleVision). Jest to zespół środków technicznych i programowych przeznaczony do obserwowania, wykrywania, rejestrowania i sygnalizowania nienormalnych warunków wskazujących na istnienie niebezpieczeństwa. W skład ich (zależnie od konfiguracji) mogą wchodzić następujące urządzenia:

- kamery telewizyjne wewnętrzne lub zewnętrzne, czarno-białe lub kolorowe,
- obiektywy,
- monitory,
- cyfrowe rejestratory wizyjne,
- zasilacze (różnych mocy oraz zawierające odpowiednie zabezpieczenia),
- klawiatury sterownicze,
- krosownice wizyjne.

Każde z wymienionych rozwiązań ma swoje zalety i wady. Po analizie ich można stwierdzić, że bardzo dobre właściwości ma zintegrowany system bezpieczeństwa w którym zastosowano do detekcji intruzów dwa wymienione systemy (tj. kabel światłowodowy i system monitoringu wizyjnego). Ich współdziałanie pozwala zwiększyć prawdopodobieństwo wykrycia intruza [10,12]. Oczywiście taki system może być w przyszłości uzupełniony o innego rodzaju podsystemy (np. aktywne bariery podczerwieni, bariery mikrofalowe, itd.).

Analiza niezawodnościowo-eksploatacyjna zintegrowanego systemu ochrony peryferyjnej

Na rys. 1 zaprezentowano hipotetyczny port lotniczy. Jest to teren na którym rozmieszczone są budynki wykorzystywane podczas procesu transportowego. Wobec rozległości obszaru, który ma być chroniony a jednocześnie dość skomplikowanego rozmieszczenia obiektów w tym obszarze, podjęto decyzję o zwróceniu szczególnej uwagi na ochronę peryferyjną. Pozwoli to na wykrycie osób nieuprawnionych (które chciały by się dostać na teren portu lotniczego) już w momencie przekraczania granicy obszaru chronionego (czyli ogrodzenia). Dlatego też zastosowano system monitoringu wizyjnego i kabel światłowodowy.

Przeprowadzając analizę funkcjonowania [11,14] zintegrowanego system ochrony peryferyjnej portu lotniczego w którym zastosowano do detekcji intruzów dwa podsystemy (kabel światłowodowy i monitoring wizyjny), można zilustrować relacje zachodzące w nim, tak jak przedstawia to rys. 2.

Uszkodzenie podsystemu wykorzystującego kabel światłowodowy powoduje przejście ze stanu pełnej zdatności S_{PZ} do stanu zagrożenia bezpieczeństwa S_{ZB1}. Przywrócenie stanu zdatności temu podsystemowi powoduje przejście ze stanu zagrożenia bezpieczeństwa S_{ZB1} do stanu pełnej zdatności S_{PZ}. W przypadku gdy zintegrowanego system ochrony peryferyjnej portu lotniczego znajduje się w stanie S_{ZB1} i nastąpi uszkodzenie podsystemu monitoringu wizyjnego, to następuje przejście do stanu zawodności bezpieczeństwa S_B.

Uszkodzenie podsystemu monitoringu wizyjnego powoduje przejście ze stanu pełnej zdatności S_{PZ} do stanu zagrożenia bezpieczeństwa S_{ZB2}. Przywrócenie stanu zdatności temu podsystemowi powoduje przejście ze stanu zagrożenia bezpieczeństwa S_{ZB2} do stanu pełnej zdatności S_{PZ}. W przypadku gdy zintegrowanego system ochrony peryferyjnej portu lotniczego znajduje się w stanie S_{ZB2} i nastąpi uszkodzenie podsystemu wykorzystującego kabel światłowodowy następuje przejście do stanu zawodności bezpieczeństwa S_B.

W rozważaniach pominięto (jako bardzo mało prawdopodobne) możliwość jedno-

System przedstawiony na rys. 2 może być opisany następującymi równaniami Kołmogorowa-Chapmana:

$$\begin{aligned} R_0'(t) &= -\lambda_{ZB1}\cdot R_0(t) + \mu_{PZ1}\cdot Q_{ZB1}(t) - \lambda_{ZB2}\cdot R_0(t) + \mu_{PZ2}\cdot Q_{ZB2}(t) \\ Q_{ZB1}'(t) &= \lambda_{ZB1}\cdot R_0(t) - \mu_{PZ1}\cdot Q_{ZB1}(t) - \lambda_{B1}\cdot Q_{ZB1}(t) \\ Q_{ZB2}'(t) &= \lambda_{ZB2}\cdot R_0(t) - \mu_{PZ2}\cdot Q_{ZB2}(t) - \lambda_{B2}\cdot Q_{ZB2}(t) \\ Q_B'(t) &= \lambda_{B1}\cdot Q_{ZB1}(t) + \lambda_{B2}\cdot Q_{ZB2}(t) \end{aligned} \tag{1}$$

Przyjmując warunki początkowe:

$$\begin{aligned} R_0(0) &= 1 \\ Q_{ZB1}(0) &= Q_{ZB2}(0) = Q_B(0) = 0 \end{aligned} \tag{2}$$

i stosując przekształcenie Laplace'a otrzymujemy następujący układ równań liniowych:

$$\begin{aligned} s\cdot R_0^*(s) - 1 &= -\lambda_{ZB1}\cdot R_0^*(s) + \mu_{PZ1}\cdot Q_{ZB1}^*(s) - \lambda_{ZB2}\cdot R_0^*(s) + \mu_{PZ2}\cdot Q_{ZB2}^*(s) \\ s\cdot Q_{ZB1}^*(s) &= \lambda_{ZB1}\cdot R_0^*(s) - \mu_{PZ1}\cdot Q_{ZB1}^*(s) - \lambda_{B1}\cdot Q_{ZB1}^*(s) \\ s\cdot Q_{ZB2}^*(s) &= \lambda_{ZB2}\cdot R_0^*(s) - \mu_{PZ2}\cdot Q_{ZB2}^*(s) - \lambda_{B2}\cdot Q_{ZB2}^*(s) \\ s\cdot Q_B^*(s) &= \lambda_{B1}\cdot Q_{ZB1}^*(s) + \lambda_{B2}\cdot Q_{ZB2}^*(s) \end{aligned} \tag{3}$$

Przekształcając go otrzymujemy zapis w ujęciu schematycznym:

$$R_0^*(s) = \frac{(s+\mu_{PZ1}+\lambda_{B1})\cdot(s+\mu_{PZ2}+\lambda_{B2})}{\left[\begin{array}{l}(s+\lambda_{ZB1}+\lambda_{ZB2})\cdot(s+\mu_{PZ1}+\lambda_{B1})\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \\ -\mu_{PZ1}\cdot\lambda_{ZB1}\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \mu_{PZ2}\cdot\lambda_{ZB2}\cdot(s+\mu_{PZ1}+\lambda_{B1})\end{array}\right]}$$

$$Q_{ZB1}^*(s) = \lambda_{ZB1}\cdot\frac{s+\mu_{PZ2}+\lambda_{B2}}{\left[\begin{array}{l}(s+\lambda_{ZB1}+\lambda_{ZB2})\cdot(s+\mu_{PZ1}+\lambda_{B1})\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \\ -\mu_{PZ1}\cdot\lambda_{ZB1}\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \mu_{PZ2}\cdot\lambda_{ZB2}\cdot(s+\mu_{PZ1}+\lambda_{B1})\end{array}\right]} \tag{4}$$

$$Q_{ZB2}^*(s) = \lambda_{ZB2}\cdot\frac{s+\mu_{PZ1}+\lambda_{B1}}{\left[\begin{array}{l}(s+\lambda_{ZB1}+\lambda_{ZB2})\cdot(s+\mu_{PZ1}+\lambda_{B1})\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \\ -\mu_{PZ1}\cdot\lambda_{ZB1}\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \mu_{PZ2}\cdot\lambda_{ZB2}\cdot(s+\mu_{PZ1}+\lambda_{B1})\end{array}\right]}$$

$$Q_B^*(s) = \frac{\left[\lambda_{B1}\cdot\lambda_{ZB1}\cdot(s+\mu_{PZ2}+\lambda_{B2})\right] + \left[\lambda_{B2}\cdot\lambda_{ZB2}\cdot(s+\mu_{PZ1}+\lambda_{B1})\right]}{s\cdot\left[\begin{array}{l}(s+\lambda_{ZB1}+\lambda_{ZB2})\cdot(s+\mu_{PZ1}+\lambda_{B1})\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \\ -\mu_{PZ1}\cdot\lambda_{ZB1}\cdot(s+\mu_{PZ2}+\lambda_{B2}) - \mu_{PZ2}\cdot\lambda_{ZB2}\cdot(s+\mu_{PZ1}+\lambda_{B1})\end{array}\right]}$$

czesnego wystąpienia uszkodzenia podsystemu wykorzystującego kabel światłowodowy i podsystemu monitoringu wizyjnego.

Przeprowadzając dalszą analizę matematyczną otrzymuje się zależności pozwalające na wyznaczenie prawdopodobieństw przebywania zintegrowanego system ochrony peryferyjnej portu lotniczego w stanach: pełnej zdatności S_{PZ}, zagrożenia bezpieczeństwa S_{ZB1} i S_{ZB2} oraz zawodności bezpieczeństwa S_B. Stosując zaprezentowaną metodykę istnieje możliwość porównania różnego rodzaju rozwiązań i wyboru optymalnego przy założonych kryteriach.

Wnioski

Port lotniczy jest obiektem, który posiada wszystkie założenia i cele terroryzmu, czyli duże skupiska osób, niekontrolowany dostęp do stref ogólnodostępnych oraz ogromne zniszczenia w przypadku przeprowadzonego zamachu. Dlatego też bardzo istotne jest stosowanie najnowocześniejszych systemów bezpieczeństwa. W artykule zaprezentowano przykładowe rozwiązania z zakresu ochrony peryferyjnej obiektów o znaczeniu strategicznym. Dokonano także analizy niezawodnościowo-eksploatacyjnej zintegrowanego systemu ochrony peryferyjnej portu lotniczego. Uzyskane zależności pozwalają obliczyć wartości prawdopodobieństw przebywania systemu w wyróżnionych stanach. Stosując je, można porównać różnego rodzaju rozwiązania i dokonać wyboru optymalnego przy założonych kryteriach wstępnych. ◀

Materiały źródłowe

[1] Balejko M., Rosiński A.: Bezpieczeństwo w porcie lotniczym. XXVII Międzynarodowa Konferencja Naukowo – Techniczna EKOMILITARIS 2013, Zakopane 2013.

[2] Fischer, Halibozek, Walters: Introduction to Security. Butterworth-Heinemann, 2012.

[3] Fries R., Chowdhury M., Brummond J.: Transportation infrastructure security utilizing inteligent transportation systems. John Wiley & Sons, New Jersey 2009.

[4] Hołyst B.: Terroryzm. Tom 1 i 2. Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.

[5] Kałużny P.: Telewizyjne systemy dozorowe. WKiŁ, Warszawa 2008.

[6] Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.

[7] Rozporządzenie Komisji (UE) nr 185/2010 z dnia 4 marca 2010 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych norm ochrony lotnictwa cywilnego.

[8] Rozporządzenie Rady Ministrów z dnia 19 czerwca 2007 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego realizującego zasady ochrony lotnictwa.

[9] Rządowe Centrum Bezpieczeństwa: „Narodowy program ochrony infrastruktury krytycznej. Załącznik 1: Charakterystyka systemów infrastruktury krytycznej". Warszawa 2013.

[10] Siergiejczyk M., Rosiński A.: Analiza poziomu bezpieczeństwa systemu ochrony peryferyjnej portu lotniczego. Prace Naukowe Politechniki Warszawskiej. Transport. z. 102, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2014.

[11] Siergiejczyk M., Rosiński A.: Analysis of power supply maintenance in transport telematics system. „Solid State Phenomena" vol. 210 (2014).

[12] Siergiejczyk M., Rosiński A.: Metodyka modelowania poziomu bezpieczeństwa systemów ochrony peryferyjnej. XXVIII Międzynarodowa Konferencja Naukowo – Techniczna EKOMILITARIS 2014, Zakopane 2014.

[13] Siergiejczyk M., Rosiński A.: Reliability analysis of electronic protection systems using optical links. Monografia „Dependable Computer Systems" pod redakcją Wojciecha Zamojskiego, Janusza Kacprzyka, Jacka Mazurkiewicza, Jarosława Sugiera i Tomasza Walkowiaka, wydana jako monograficzna seria wydawnicza – „Advances in intelligent and soft computing", Vol. 97. Wydawca: Springer-Verlag, Berlin Heidelberg 2011.

[14] Siergiejczyk M., Rosiński A.: Reliability analysis of power supply systems for devices used in transport telematic systems. Monografia „Modern Transport Telematics" pod redakcją Jerzego Mikulskiego, wydana jako monograficzna seria wydawnicza – „Communications in Computer and Information Science", Vol. 239. Wydawca: Springer-Verlag, Berlin Heidelberg 2011.

[15] Siergiejczyk M., Rosiński A.: Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego. Monografia „Rewaluacja bezpieczeństwa publicznego" pod redakcją naukową Tadeusza Zaborowskiego. Wydawca: Instytut Badań i Ekspertyz Naukowych w Gorzowie Wlkp., Gorzów Wlkp. 2011.