ISSN 1232-3829
tts 10/2013
Technika Transportu Szynowego koleje ▪ tramwaje ▪ metro

SIERGIEJCZYK Mirosław, ROSIŃSKI Adam

SYSTEMY OCHRONY PERYFERYJNEJ OBIEKTÓW TRANSPORTOWYCH INFRASTRUKTURY KRYTYCZNEJ

Streszczenie

W artykule przedstawiono zagadnienia związane z systemami bezpieczeństwa stosowanymi do ochrony infrastruktury krytycznej, ze szczególnym uwzględnieniem ich zastosowania w transporcie. Zaprezentowano też koncepcję systemu ochrony peryferyjnej bazy transportowej. Dla zaproponowanego rozwiązania podano zalety i wady.

WSTĘP

Według „Narodowego Programu Ochrony Infrastruktury Krytycznej" w Rzeczypospolitej Polskiej w skład infrastruktury krytycznej wchodzi 11 systemów. Mają one kluczowe znaczenie dla bezpieczeństwa państwa i jego obywateli [1,9]. Jednocześnie też zapewniają sprawne funkcjonowanie organów administracji publicznej, a także instytucji i przedsiębiorców. W skład infrastruktury krytycznej zaliczamy następujące systemy [5]:

– 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).

Istotną rolę wśród wymienionych systemów zajmuje transport. Według [5] 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 [6,7]. W tym celu wykorzystuje się różne rozwiązania [8].

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

– sygnalizacji włamania i napadu [3],

– sygnalizacji pożaru,
– kontroli dostępu [4],
– monitoringu wizyjnego [2],
– 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.

Istotnym elementem systemów alarmowych są systemy transmisji alarmu stanowiące urządzenia albo sieci do przekazywania informacji o stanie jednego lub więcej systemów alarmowych do jednego lub kilku alarmowych centrów odbiorczych.

Najkorzystniej jest zastosować elektroniczne systemy bezpieczeństwa i odpowiednie służby ochrony, które powiązane są między sobą poprzez odpowiednie procedury działania. W artykule została zaprezentowana koncepcja ochrony peryferyjnej obiektów transportowych, rozważanych jako element infrastruktury krytycznej.

1. SYSTEMY SYGNALIZACJI ZAGROŻEŃ

Jak wspomniano we wstępie występują różnego rodzaju elektroniczne systemy bezpieczeństwa, które mogą być zastosowane w ochronie obiektów transportowych. Można je podzielić według zastosowań i zjawisk przeciwko jakim są stosowane. W niniejszym rozdziale zostaną one ogólnie scharakteryzowane.

1.1. System sygnalizacji włamania i napadu

System Sygnalizacji Włamania i Napadu (SSWiN) ma za zadanie wykryć i zasygnalizować stan zagrożenia mienia i osób. Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements”, która ma jednocześnie status Polskiej Normy PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Wymagania systemowe” [3], zawiera wykaz części składowych (elementów), które powinien zawierać SSWiN: centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu, zasilacz podstawowy, zasilacz rezerwowy. Centrala alarmowa stanowi „serce” systemu. Do niej przesyłane są informacje o stanie poszczególnych linii dozorowych (np. czujki), linii wyjściowych (np. obciążenia wyjść) czy dane wprowadzane przez użytkownika lub konserwatora (a wcześniej podczas instalacji systemu – instalatora). W zależności od typu centrali alarmowej informacje mogą być przesyłane bezpośrednio do płyty głównej centrali alarmowej lub też do modułów, realizujących określone funkcje (np. rozszerzeniowe wejść, rozszerzeniowe wyjść, interfejsy drukarek, itd.).

1.2. System monitoringu wizyjnego

Systemy monitoringu wizyjnego (CCTV) 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 [2]:
– 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.

1.3. System kontroli dostępu

System kontroli dostępu (SKD) zwany również systemem sterowania dostępem to zespół urządzeń i oprogramowania, które mają za zadanie:
– identyfikację osób albo pojazdów, uprawnionych do przekroczenia granicy obszaru zastrzeżonego oraz umożliwienie im wejścia/wyjścia,
– niedopuszczenie do przejścia przez osoby albo pojazdy nieuprawnione granicy obszaru zastrzeżonego,
– wytworzenie sygnału alarmowego informującego o próbie przejścia osoby albo pojazdu nieuprawnionego przez granicę obszaru zastrzeżonego.

1.4. System ochrony terenów zewnętrznych

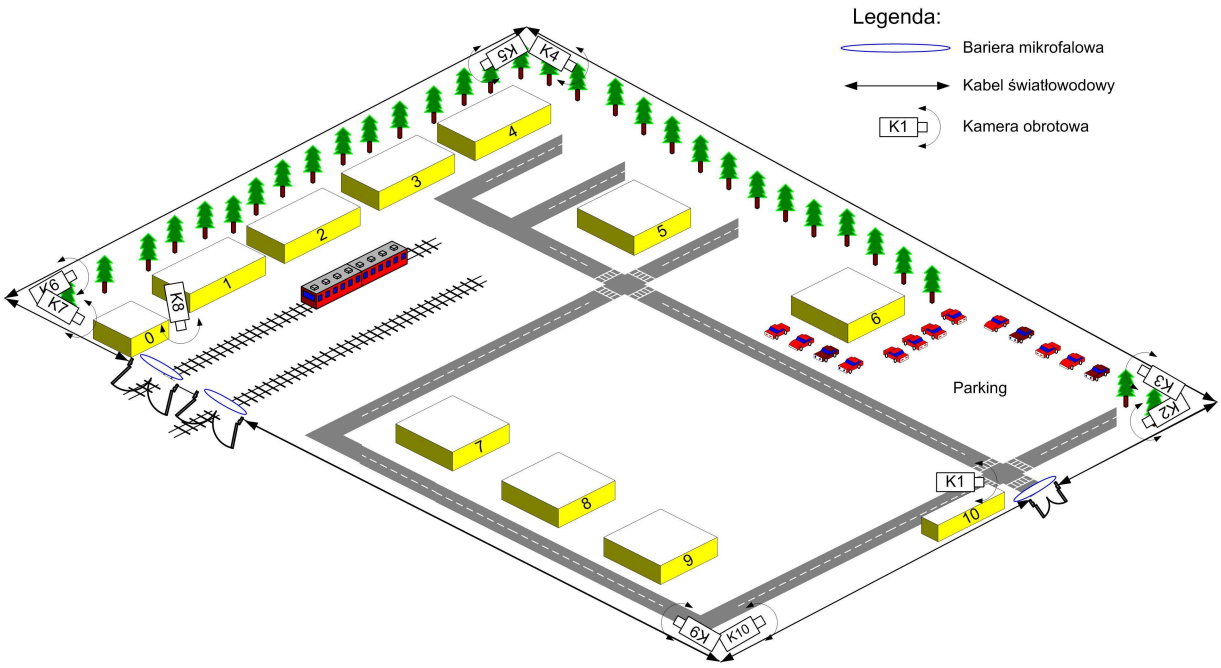
Systemy ochrony terenów zewnętrznych mają za zadanie zabezpieczenie obiektów przestrzennych. Istotne staje się wykrycie ingerencji osób nieuprawnionych. Celem jest więc zminimalizowanie wpływu potencjalnych strat w przypadku wystąpienia zagrożenia dla chronionego obiektu. Wcześniejsze wykrycie miejsca takiego incydentu pozwala na szybszą interwencję służb ochrony i podjęcie racjonalnych działań zmierzających do zminimalizowania zagrożenia.

Współczesne systemy ochrony terenów zewnętrznych obiektów o specjalnym przeznaczeniu można podzielić na [10]:
– systemy ogrodzeniowe instalowane na wewnętrznym ogrodzeniu obwodnicy,
– naziemne systemy ochrony zewnętrznej,
– ziemne systemy ochrony zewnętrznej.

2. KONCEPCJA OCHRONY PERYFERYJNEJ OBIEKTÓW TRANSPORTOWYCH

Obiekty transportowe (zarówno stacjonarne jak i ruchome) spełniają istotną rolę w funkcjonowaniu gospodarki kraju. Dlatego też, jako elementy infrastruktury krytycznej, powinny podlegać szczególnej ochronie. Systemy bezpieczeństwa tam stosowane muszą być tak zaprojektowane by spełniały wymagania inwestora, a jednocześnie też jak najpełniej zgadzały się z wymaganiami zawartymi w odpowiednich normach.

Na rys. 1 zaprezentowano hipotetyczną bazę transportową. Jest to teren na którym rozmieszczone są budynki (numery od 1 do 9) wykorzystywane podczas procesu transportowego. Budynki o numerach „0” i „10” pełnią rolę portierni, na których odbywa się kontrola pojazdów wjeżdżających i wyjeżdżających z chronionego obszaru. Pojazdami mogą być zarówno samochody, jak też pociągi. Część terenu w pobliżu budynków 7, 8 i 9 pełni rolę placu na którym przechowywane są kontenery dostarczone przez pociągi i przewożone następnie przez pojazdy ciężarowe. Wobec rozległości obszaru, który ma być chroniony a jednocześnie dość skomplikowanego rozmieszczenia budynków 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 bazy transportowej) już w momencie przekraczania granicy obszaru chronionego (czyli ogrodzenia).



Rys. 1. Widok bazy transportowej z zastosowanymi systemami bezpieczeństwa
Źródło: [opracowanie własne]

Zapewnienie odpowiedniego poziomu bezpieczeństwa przedstawionej bazy transportowej wymaga zastosowania poszczególnych systemów bezpieczeństwa, takich jak: sygnalizacji włamania i napadu, sygnalizacji pożaru, kontroli dostępu, monitoringu wizyjnego, ochrony terenów zewnętrznych. Szczegółowy opis ich wdrożenia w obiekcie wymagałby bardzo wielu uszczegółowień i wobec ograniczonej objętości artykułu, zostanie przedstawiona tylko koncepcja ochrony peryferyjnej.

Ochrona peryferyjna obiektu jakim jest zaprezentowana baza transportowa pozwala na użycie wielu możliwych do zastosowania technologii wykrycia osób nieuprawnionych do przekroczenia ogrodzenia. Wśród nich można wyróżnić m.in. [10]:

- systemy ogrodzeniowe instalowane na wewnętrznym ogrodzeniu obwodnicy:
  - kablowe tryboelektryczne,
  - kablowe mikrofonowe,
  - kablowe elektromagnetyczne,
  - kablowe światłowodowe (natężeniowe i interferometryczne),
  - czujniki piezoelektryczne punktowe,
  - ogrodzenie aktywne – z wmontowanymi czujnikami mechaniczno-elektrycznymi,
- naziemne systemy ochrony zewnętrznej:
  - aktywne bariery mikrofalowe,
  - aktywne bariery podczerwieni,
  - pasywne czujki podczerwieni,
  - dualne czujki,
  - radary mikrofalowe,
  - radary laserowe,
- ziemne systemy ochrony zewnętrznej:
  - kablowe elektryczne aktywne (pole elektryczne),
  - kablowe magnetyczne pasywne (pole magnetyczne),
  - kablowe światłowodowe naciskowe,
  - kablowe elektromagnetyczne naciskowe,

- czujniki sejsmiczne.

Każde z wymienionych rozwiązań ma swoje zalety i wady. Po analizie ich można stwierdzić, że bardzo dobre właściwości ma system w którym zastosowano do detekcji intruzów kabel światłowodowy. Jedną z jego zalet jest odporność na zakłócenia elektromagnetyczne, a tym samym niewrażliwość na tego typu zakłócenia wygenerowane (celowo lub przypadkowo) przez obce źródła.

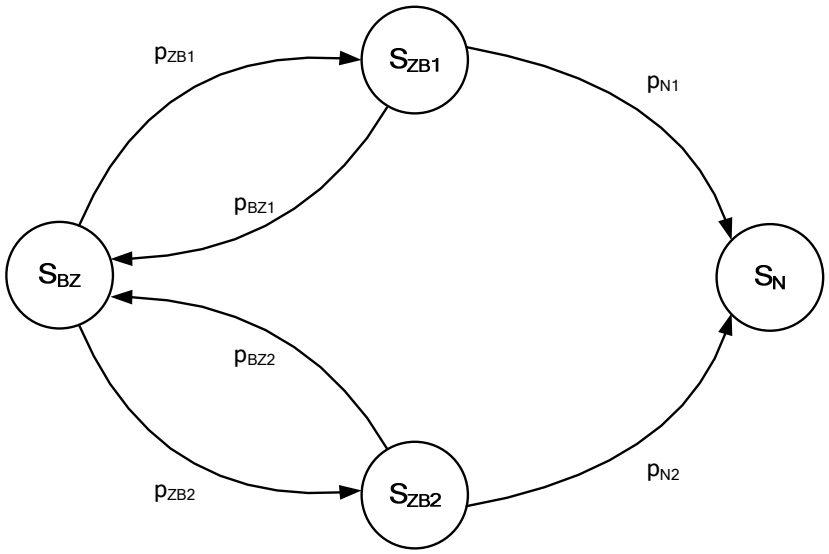
Do ochrony bram służących do wjazdu na teren bazy transportowej zaproponowano bariery mikrofalowe. Były by one wykorzystywane w czasie, gdy wjazdy na teren byłyby zamknięte. W pozostałych porach dnia osoby pełniące dyżur w budynkach „0" i „10" dokonywały by kontroli oraz weryfikacji pojazdów i osób wjeżdżających i wyjeżdżających z terenu bazy transportowej.

Uzupełnieniem wymienionych systemów bezpieczeństwa będzie system monitoringu wizyjnego. Zastosowanie jego pozwoli na zobrazowanie sytuacji jaka występuje na chronionym obszarze. Wobec rozległości terenu zaproponowano użycie kolorowych kamer obrotowych z funkcją „zoom". Umożliwi to ukazania szczegółów w przypadku zaistnienia sytuacji potencjalnie niebezpiecznych. Kamery zostaną umieszczone tak, by móc widzieć teren w pobliżu ogrodzenia (kamery o numerach 2÷7, 9 i 10). Zastosowany zostanie filtr analizujący obraz w postaci przekroczenia wirtualnej granicy. Umożliwi to automatyczne alarmowanie w sytuacji gdy osoba przekroczy ogrodzenie. Kamery zlokalizowane w pozycjach 1 i 8 obserwują bezpośrednio wjazdy na teren bazy logistycznej. Obraz z nich uzyskany może być w przyszłości wykorzystywany do rozpoznawania tablic rejestracyjnych pojazdów (kamera 1) oraz oznaczeń kontenerów na platformach wagonów kolejowych (kamera 8).

Dane uzyskane z systemów ochrony peryferyjnej oraz systemów monitoringu wizyjnego zostaną przekazane do centrum zarządzania i nadzoru. Tam też będą przesyłane informacje z pozostałych systemów bezpieczeństwa. Wobec dużej liczby różnorodnych systemów przewiduje się wykorzystanie wydzielonych sieci teleinformatycznych, które będą użyte tylko dla systemów bezpieczeństwa.

3. ANALIZA SKUTECZNOŚCI FUNKCJONOWANIA SYSTEMU OCHRONY PERYFERYJNEJ ZAPROPONOWANEJ KONCEPCJI

Zaproponowana koncepcja ochrony peryferyjnej obiektu transportowego zakłada wykorzystanie w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dwóch systemów: monitoringu wizyjnego i kabla światłowodowego. Analizując proces detekcji osób nieuprawnionych do przekroczenia granicy obszaru chronionego, można zobrazować zaistniałe sytuacje, tak jak przedstawiono to na rys. 2. Stan braku zagrożenia bezpieczeństwa S_{BZ} jest w stanem w którym oba systemy detekcji ochrony peryferyjnej nie wykryły zagrożenia. Stan zagrożenia bezpieczeństwa 1 S_{ZB1} jest stanem w którym pierwszy system ochrony peryferyjnej (kabel światłowodowy) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu S_{BZ} do stanu S_{ZB1} z prawdopodobieństwem p_{ZB1}). Stan zagrożenia bezpieczeństwa 2 S_{ZB2} jest stanem w którym drugi system ochrony peryferyjnej (monitoring wizyjny) wykrył potencjalne zagrożenie (zatem następuje przejście ze stanu S_{BZ} do stanu S_{ZB2} z prawdopodobieństwem p_{ZB2}). Będąc odpowiednio w stanach S_{ZB1} i S_{ZB2} , w przypadku stwierdzenia braku zagrożenia następuje przejście do stanu S_{BZ} odpowiednio z prawdopodobieństwami równymi p_{BZ1} i p_{BZ2}. Jeśli system ochrony peryferyjnej znajduje się w stanie S_{ZB1} i nastąpi potwierdzenie zagrożenia przez drugi system detekcji, wówczas z prawdopodobieństwem p_{N1} następuje przejście do stanu niebezpieczeństwa S_N. Jeśli system ochrony peryferyjnej znajduje się w stanie S_{ZB2} i nastąpi potwierdzenie zagrożenia przez pierwszy system detekcji, wówczas z prawdopodobieństwem p_{N2} następuje przejście do stanu niebezpieczeństwa S_N.



Rys. 2. Relacje w systemie ochrony peryferyjnej
Źródło: [opracowanie własne]

Dla grafu przejść przedstawionego na rys. 2 można zapisać następujące równania:

$$P_{SBZ} = p_{BZ1} \cdot P_{SZB1} + p_{BZ2} \cdot P_{SZB2}$$
$$P_{SZB1} = p_{ZB1} \cdot P_{SBZ}$$
$$P_{SZB2} = p_{ZB2} \cdot P_{SBZ}$$
$$P_{SN} = p_{N1} \cdot P_{SZB1} + p_{N2} \cdot P_{SZB2}$$

Oczywiście:

$$P_{SBZ} + P_{SZB1} + P_{SZB2} + P_{SN} = 1$$

Stosując odpowiednie przekształcenia matematyczne, można wyznaczyć wartości prawdopodobieństw przebywania w wyróżnionych stanach. Umożliwi to ocenę skuteczności funkcjonowania zaproponowanego rozwiązania. W przyszłości możliwe jest także wykorzystanie opracowanej metodologii analizy funkcjonowania systemów ochrony peryferyjnej do porównania różnego rodzaju rozwiązań i wyboru optymalnego przy założonych warunkach początkowych.

PODSUMOWANIE

Podsumowując zaprezentowane rozwiązania można stwierdzić, iż istnieje bardzo wiele różnorodnych rozwiązań z zakresu systemów bezpieczeństwa, które pozwalają na zwiększenie poziomu bezpieczeństwa obiektów transportowych. Ponieważ są one zaliczane do infrastruktury krytycznej, to powinno stosować się różne środki techniczne i organizacyjne w celu ochrony przed różnymi zagrożeniami. W artykule ukazano wykorzystanie systemów ochrony peryferyjnej (w postaci kabli światłowodowych i barier mikrofalowych) do ochrony terenów bazy transportowej. Zastosowane tylko ich nie w pełnym zakresie spełnia wymagania odnośnie bezpieczeństwa. Dlatego też zastosowano system monitoringu wizyjnego. Pozwoli to m.in. na rejestracje zdarzeń i późniejsze ich wykorzystanie jako materiał dowodowy. Wadą zaproponowanych rozwiązań jest stosunkowo duży koszt ich wdrożenia, jednakże możliwe jest zastosowanie ich (systemu monitoringu wizyjnego) także w funkcjach nie związanych bezpośrednio z bezpieczeństwem.

BIBLIOGRAFIA

1. Hołyst B., Terroryzm. Tom 1 i 2. Wydawnictwa Prawnicze LexisNexis, Warszawa, 2011.
2. Kałużny P., Telewizyjne systemy dozorowe. WKiŁ, Warszawa, 2008.
3. Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
4. Norma PN-EN 50133-1:2007 - Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część 1: Wymagania systemowe.
5. Rządowe Centrum Bezpieczeństwa: „Narodowy program ochrony infrastruktury krytycznej. Załącznik 1: Charakterystyka systemów infrastruktury krytycznej". Warszawa 2013.
6. Siergiejczyk M., Gago S., Koncepcja systemu monitorowania i nadzoru w węźle kolejowym. VI Międzynarodowa Konferencja Naukowo-Techniczna LOGITRANS 2009, Szczyrk, 2009.
7. Siergiejczyk M., Gago S., Public Safety Issues in Rail Transport. Polish Journal of Environmental Studies. ISSN 1230-1485.Vol 17, No 3C (2008). HARD Publishing Company, Olsztyn 2008.
8. Siergiejczyk M., Rosiński A., Wykorzystanie wybranych elementów telematyki transportu w zapewnieniu bezpieczeństwa publicznego. IV Międzynarodowa Konferencja Naukowa „Bezpieczeństwo Publiczne BP'11", Poznań, 2011.
9. Siergiejczyk M., Rosiński A., Zagrożenia podczas podróży w transporcie kolejowym. V Międzynarodowa Konferencja Naukowa „Bezpieczeństwo Publiczne BP'12", Poznań 2012.
10. Szulc W., Rosiński A., Metody ochrony obwodowej obiektów. XXIV Międzynarodowa Konferencja Naukowo – Techniczna EKOMILITARIS 2010, Zakopane 2010.

SYSTEMS OF PERIPHERAL PROTECTION OF CRITICAL INFRASTRUCTURE OF TRANSPORT OBJECTS

Abstract

The article presents the issues related to security systems used to protect critical infrastructure, with particular emphasis on their use in transport. The paper presents a concept of system of protection of the peripheral transport base. For the proposed solution are given advantages and disadvantages.

Autorzy:

prof. nzw. dr hab. inż. **Mirosław Siergiejczyk** – Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie

dr inż. **Adam Rosiński** – Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie