TRANSCOMP – XIV INTERNATIONAL CONFERENCE
COMPUTER SYSTEMS AIDED SCIENCE, INDUSTRY AND TRANSPORT

4Systemy bezpieczeństwa,
Systemy Sygnalizacji Włamania i Napadu,
Ochrona obwodowa

Waldemar SZULC[1]
Adam ROSIŃSKI[2]

OCHRONA OBWODOWA OBIEKTÓW TRANSPORTOWYCH O ZNACZENIU STRATEGICZNYM

Miejsce wykrywania osoby nieuprawnionej ma wpływ na ewentualne straty 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. W referacie przedstawiono koncepcje zintegrowanego, elektronicznego systemu bezpieczeństwa do ochrony obiektów transportowych o znaczeniu strategicznym z punktu widzenia zapewnienia ciągłości działania transportu krajowego. Zastosowano w nim m.in. różne metody ochrony obwodowej chronionego obiektu. Opisano także techniki ochrony obiektów rozległych terytorialnie ze szczególnym uwzględnieniem ich specyfiki.

PERIMETER SAFEGUARD OF STRATEGICALLY IMPORTANT OBJECT OF TRANSPORTATION

The place where an unauthorized person is detected has an effect on possible losses in case of danger for safeguarded objects. An early detection of the place of such an incident allows for a quick intervention of the security service and for bringing in a rational action to minimalize the risk. In this paper there is presented a concept of an integrated electronic security system for object of transportation strategically important from the point of view of the country transportation system. Various perimeter safeguard methods are applied in this system. Additionally, safeguard systems for objects covering large areas are described.

1. WSTĘP

Obiektem zabezpieczenia obwodowego jest obiekt przestrzenny. Istotne staje się wykrycie ingerencji osób nieuprawnionych. Celem jest więc minimalizowanie wpływu potencjalnych strat w przypadku wystąpienia zagrożenia dla chronionego obiektu. Wcześniejsze wykrycie miejsca takiego incydentu pozwala na szybszą interwencję służb

[1] Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej, Polska, 03-772 Warszawa, ul. Kawęczyńska 36, tel. 22 5900829, e-mail: waldemar.szulc@mac.edu.pl
[2] Politechnika Warszawska, Wydział Transportu, Zakład Telekomunikacji w Transporcie, Polska, 00-662 Warszawa, ul. Koszykowa 75, tel.: 22 2347038, e–mail: adro@it.pw.edu.pl

ochrony i podjęcie racjonalnych działań zmierzających do zminimalizowania zagrożenia [2]. W referacie przedstawiono koncepcje zintegrowanego, elektronicznego systemu bezpieczeństwa do ochrony obiektów transportowych o znaczeniu strategicznym z punktu widzenia zapewnienia ciągłości działania transportu krajowego. Dla ochrony zewnętrznej stosuje się systemy peryferyjne a więc takie, które instaluje się tuż przy obiekcie i systemy obwodowe, które chronią obiekt znacznie wcześniej Zastosowano w nim m.in. różne metody ochrony obwodowej chronionego obiektu. Opisano także techniki ochrony obiektów rozległych terytorialnie ze szczególnym uwzględnieniem ich specyfiki. Do najczęściej spotykanych metod ochrony peryferyjnej i obwodowej należy zaliczyć: różne typy barier aktywnych, bariery mikrofalowe, specjalne kable światłowodowe, bardzo nowoczesne czujki zew. typu PIR (dalekiego zasięgu), systemy telemetryczne, systemy laserowe. Wszystkie wymienione metody i systemy są zwykle wspomagane bardzo rozbudowanym monitoringiem wizyjnym. Często monitoring wizyjny współpracuje z systemami oświetlenia terenu. Mogą to być systemy oświetlaczy podczerwiennych jak i klasycznego oświetlenia. Obiekty transportowe ze względu na strategiczne znaczenie wymagają starannej ochrony elektronicznej ale i fizycznej. Obiekty transportowe to: dworce kolejowe, szlaki, porty, lotniska, górki rozrządowe, placówki naukowo-badawcze, itp. Ich ochrona to bardzo poważne wyzwanie wymagające dużej wiedzy zarówno praktycznej jak i teoretycznej. Autorzy wybrali więc określony obiekt transportowy i nim zajęto się w niniejszym referacie.

Wzrastające zagrożenia w wyniku działań przestępczych skierowanych przeciwko życiu i mieniu, wymuszają coraz to nowe sposoby ochrony przeciwko tym zjawiskom. Są budowane coraz to nowsze i bardziej wyrafinowane techniczne systemy zabezpieczeń zarówno mechanicznych jak i elektronicznych. Pomimo wzrostu możliwości technicznych i powstawaniu coraz to nowych konstrukcji w dziedzinie zabezpieczenia, trudno będzie znaleźć opcję, która da 100% bezpieczeństwa chronionej substancji. Niestety pozostaje również pewien margines ryzyka powodowanego błędnym działaniom urządzeń a niestety częściej ludzi. Przyjęto jednak zasadę, że działanie wszystkich instytucji i osób zajmujących się ochroną, są ukierunkowane na zmniejszenie ryzyka zagrożenia włamania, napadu i ataków terrorystycznych.

System pełnej sygnalizacji zagrożeń tworzy się z następujących systemów wyróżnianych zależnie od wykrywanych zagrożeń, jako systemy:

- sygnalizacji włamania i napadu (SSWiN),
- sygnalizacji pożaru (SSP),
- kontroli dostępu (SKD),
- monitoringu wizyjnego (CCTV),
- ochrony terenów zewnętrznych (peryferyjny i obwodowy).

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

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

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.

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", zawiera wykaz części składowych (elementów), które powinien zawierać System Sygnalizacji Włamania i Napadu (SSWiN) [9]: centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i/lub systemów transmisji alarmu, zasilacz podstawowy, zasilacz rezerwowy. Połączenia pomiędzy elementami systemu powinny spełniać określone wymagania, a zarazem muszą także zawierać się w dopuszczalnych przez producenta parametrach. Ogólnie można je podzielić na połączenia przewodowe lub bezprzewodowe. Zaprojektowanie oraz realizacja Systemu Sygnalizacji Włamania i Napadu dla dużego i rozległego obiektu wymaga sporej wiedzy technicznej, jak również dużego doświadczenia.

2. METODY OCHRONY OBWODOWEJ

Miejsce wykrycia osoby nieuprawnionej ma wpływ na ewentualne straty w przypadku wystąpienia zagrożenia dla chronionego obiektu. Wcześniejsze zlokalizowanie takiego incydentu pozwala na szybszą interwencję służb ochrony i podjęcie racjonalnych działań zmierzających do zminimalizowania zagrożenia. Dlatego też opracowano wiele metod ochrony obwodowej obiektów o specjalnym znaczeniu [5], 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 obwodowej obiektów o specjalnym przeznaczeniu można podzielić na [4,6,7,8]:

- 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,

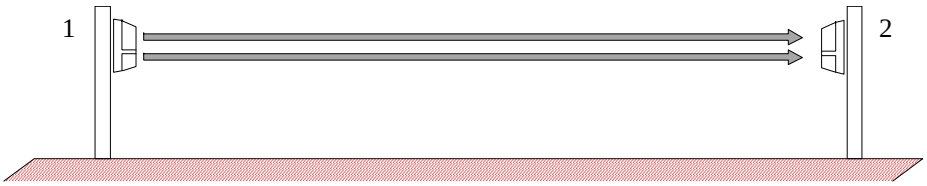
- ziemne systemy ochrony zewnętrznej:
  - kablowe elektryczne aktywne (pole elektryczne),
  - kablowe magnetyczne pasywne (pole magnetyczne),
  - kablowe światłowodowe naciskowe,
  - kablowe elektromagnetyczne naciskowe,
  - czujniki sejsmiczne.

W kolejnych podrozdziałach zostaną scharakteryzowane najczęściej stosowane rozwiązania.

2.1. Aktywne bariery podczerwieni

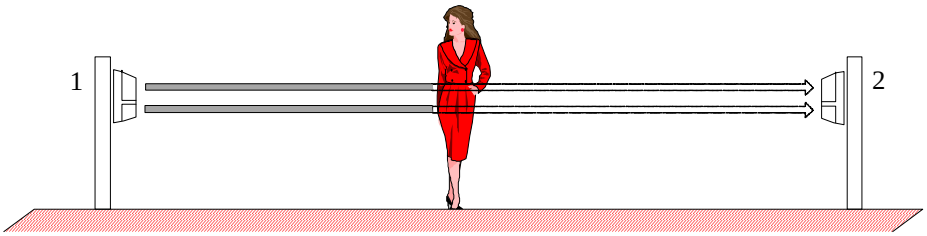
Aktywne bariery podczerwieni składają się z dwóch części: nadawczej i odbiorczej. Nadajnik emituje promieniowanie podczerwone, które normalnie jest odbierane przez odbiornik. Pojedynczy nadajnik i odbiornik stanowią tzw. tor podczerwieni. Kilka takich torów ustawionych w jednej linii tworzy tzw. barierę – przeważnie od 4 do 16 wiązek. Zasięgi działania barier zewnętrznych wynoszą od 25 m do około 200 m. Jako kryterium alarmu stosuje się bardzo często wymóg zasłonięcia dwóch wiązek (np. sąsiadujących ze sobą) w określonym czasie – pozwala to na uniknięcie fałszywych alarmów związanych z przelatującymi ptakami czy też spadającym liśćmi z drzew.

Rys. 1 przedstawia w najprostszy sposób zasadę pracy aktywnych barier podczerwieni. Aktywne tory (bariery) podczerwieni składają się z nadajnika (1) emitującego dwie (lub więcej) wiązki promieniowania podczerwieni oraz odbiornika (2), który może być umieszczony od nadajnika w określonej odległości, zależnie od modelu toru.



Rys. 1. Zasada pracy czujek aktywnych podczerwieni (1- nadajnik, 2 odbiornik)

Sygnał alarmu powstaje przy jednoczesnym przerwaniu obu wiązek, przy czym prędkość wtargnięcia w strefę chronioną i minimalny czas jej naruszenia są regulowane. Przy przerwaniu tylko jednej z wiązek np.: przez przelatującego ptaka, alarm nie jest wyzwolony. Na rys. 2 przedstawiono „naruszenie" bariery aktywnej podczerwieni (przecięcie obu wiązek).



Rys. 2. Zasada pracy czujek aktywnych podczerwieni (naruszenie obu wiązek i wywołanie alarmu)

W tabeli 1 zestawiono najczęściej spotykane instalacje barier poczerwieni aktywnej oraz ich konfiguracje. Mogą być one stosowane jako ochrona obwodowa jak i peryferyjna. Bariery aktywne dobiera się parami tak aby połączone w większe systemy nie zakłócały się wzajemnie (poz. 3, 4, 5, 6, 7, 8, 9). Zasięgi aktywnych barier podczerwieni (odległość pomiędzy nadajnikiem a odbiornikiem) wynoszą od kilku do kilkuset metrów.

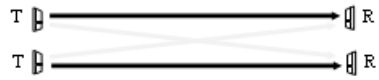
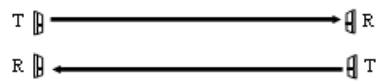
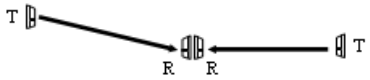
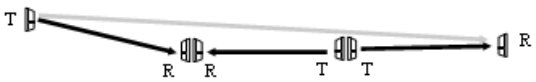
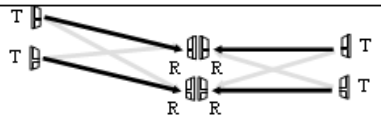
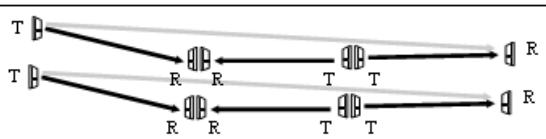
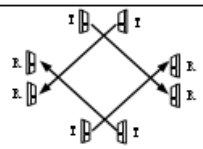
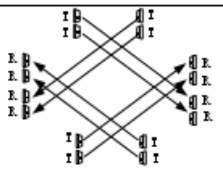
W przypadku barier ścianowych (pionowych) spotyka się do 8 wiązek podczerwieni pracujących naprzemiennie. Ilość wiązek może być programowalna.

Charakterystycznym przykładem wpływu warunków atmosferycznych jest mgła mogąca pochłaniać promienie IR (choć układ bariery może być wyposażony w system ARW (Automatyczna Regulacja Wzmocnienia).

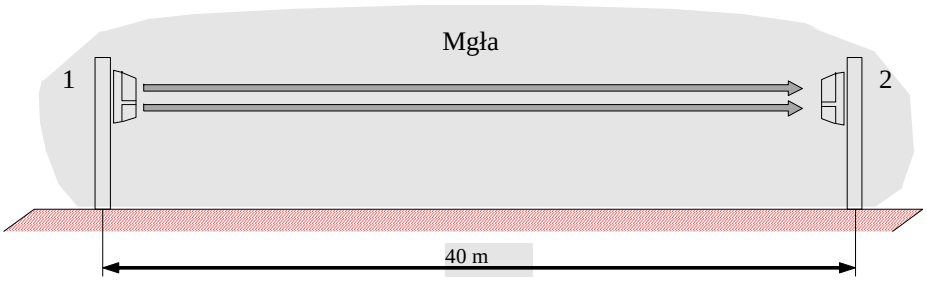
W dobrych barierach może dojść nawet do 99% utraty „mocy” sygnału a system będzie pracował poprawnie.

Na rys. 3a i 3b przedstawiono przykład bariery o zasięgu l = 40 m pracującej w warunkach mgły. Warto w warunkach mgły, deszczu lub śniegu zastąpić barierą 2 x 20 m dla zapewnienia poprawności działania. Problem dotyczy również i innych bardziej złożonych konfiguracji przedstawionych w tabeli 1.

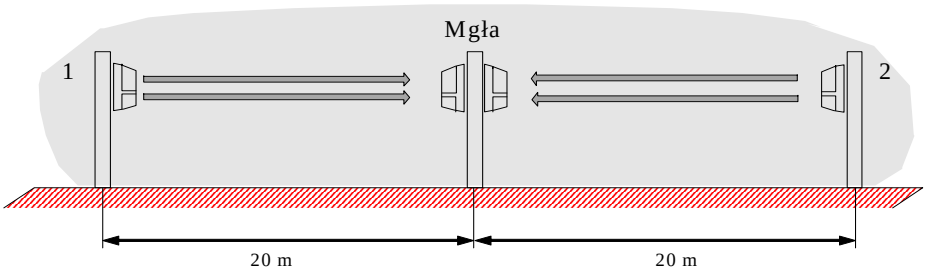
Tabela 1. Przykłady instalacji aktywnych barier podczerwieni

Przykład instalacji	T: nadajnik	R: odbiornik
1 	×	○
2 	○	○
3 	×	○
4 	○	○
5 	×	○
6 	×	○
7 	×	○
8 	○	○
9 	×	○

Na rys. 3a i 3b przedstawiono barierę aktywną o zasięgu l = 40m w przypadku wystąpienia mgły, lub padającego deszczu (śniegu). Bariera o takim zasięgu i w podanych powyżej warunkach z całą pewnością będzie źle pracowała. Może wywołać alarm. Stąd propozycja pewniejszej pracy bariery przedstawiona na rys 3b (niestety kosztowniejsze rozwiązanie). Zgodnie z tabelą 1 należy rozwiązywać konfiguracje systemów barier w trudnych warunkach atmosferycznych przyjmując zasadę przedstawiona na rys. 3a i 3b.



Rys. 3a. Aktywna bariera podczerwieni o max zasięgu l = 40m w warunkach mgły

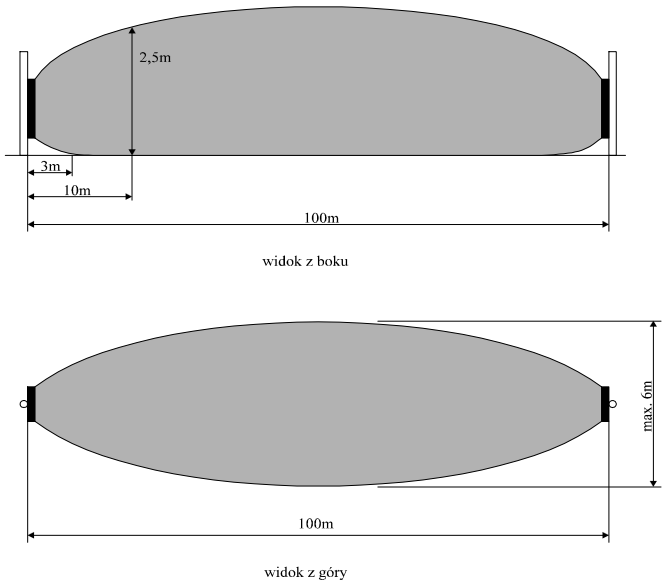


Rys. 3b. Aktywne bariery podczerwieni w warunkach mgły i propozycja poprawnej pracy

Systemy barier aktywnych mogą być instalowane zarówno w opcjach obwodowych jak i peryferyjnych. Jak wspominano powyżej w obiektach szczególnego znaczenia warto takie instalacje wspomagać monitoringiem wizyjnym z uwzględnieniem dodatkowego oświetlania terenu zarówno światłem w zakresie widzialnym jak i oświetlaczami podczerwieni.

2.2. Bariery mikrofalowe

Aktywne bariery mikrofalowe (podobnie jak aktywna bariera podczerwieni) składa się z dwóch elementów: nadajnik oraz odbiornik. Odbiornik i nadajnik montowane są naprzeciw siebie. Nadajnik emituje impuls energii mikrofalowej w stronę odbiornika, który posiada dostrojony detektor mikrofalowy. Odbiornik wykrywa zmiany sygnału wywoływane przez poruszający się obiekt. Analizując propagacje fal elektromagnetycznych pomiędzy nadajnikiem i odbiornikiem można stwierdzić, iż wymagają one dość dużej przestrzeni (dla toru detekcji) gdyż znajdujące się w pobliżu ruchome duże obiekty (np. drzewa) mogą powodować zakłócenia i nieprawidłową prace urządzenia.



Rys. 4. Przykład charakterystyki bariery mikrofalowej

Bariery mikrofalowe są stosowane jako urządzenia zewnętrzne. Bariery mikrofalowe pracują na podobnej zasadzie jak łącza mikrofalowe.

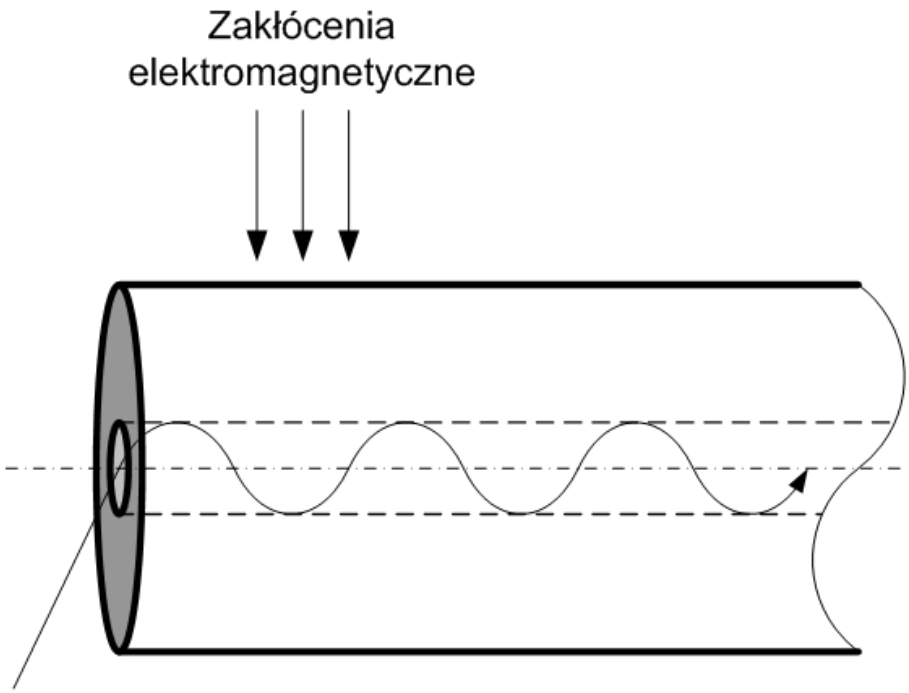
2.3. Kable tryboelektryczne

W kablu tryboelektrycznym (sensorycznym) sygnały użytkowe generowane są przez tryboelektryczny kabel koncentryczny czujnika, który posiada specjalną konstrukcję. Sygnały wywołane przez odkształcenie dielektryka (na przykład przy drganiu kabla) analizowane są przez procesor sygnału. Po spełnieniu określonych kryteriów generowany jest sygnał alarmowy (parametry alarmu są ustawiane najczęściej niezależnie dla wykrywania prób przecinania siatki oraz wspinania się po niej). Rozwiązanie to jest dość często stosowane z uwagi na szybką i prostą instalację.

Rys. 5. Kabel sensoryczny (tryboelektryczny)

2.3. Specjalne kable światłowodowe

Kabel światłowodowy jest podstawowym elementem detekcyjnym systemu. Wykrywa on nacisk lub wibracje powodowane przez intruza. Cechy światłowodu powodują, że to rozwiązanie jest całkowicie odporne na zakłócenia elektromagnetyczne. Dzięki temu, że nie przewodzi elektrycznego sygnału, można go bezpiecznie stosować w pobliżu linii energetycznych, systemów radarowych. 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. Specjalne kable światłowodowe to znakomita ochrona zarówno peryferyjna jak i obwodowa. Należy jednak pamiętać, że stosowane kable światłowodowe posiadają specjalna konstrukcję. Pozwalają na bardzo precyzyjne określenie miejsca naruszenia.

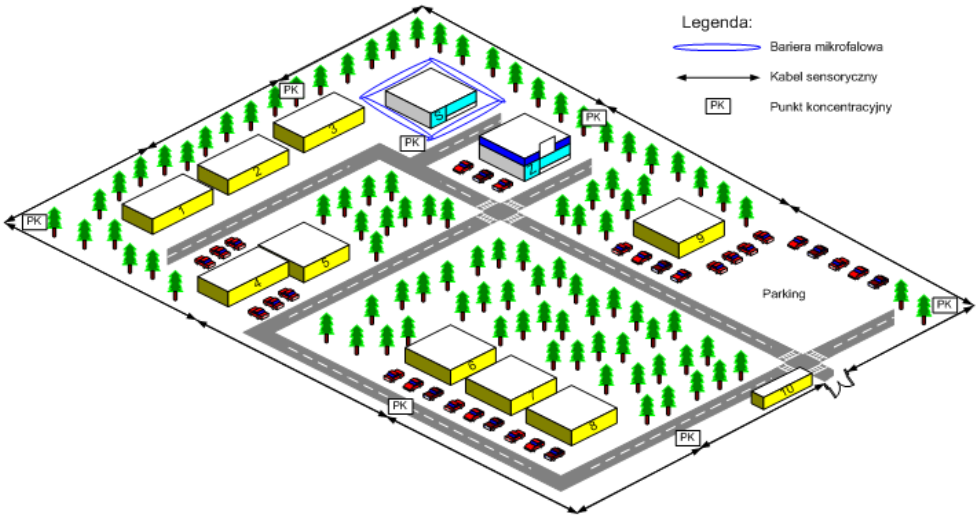


Rys. 6. Kabel światłowodowy specjalnej konstrukcji wraz z widokiem fali stojącej (pionowo oznaczono ewentualne zakłócenie)

Promień świetlny w przewodzie światłowodowym sensorycznym (np. Fiber Defender) jest odporny na efekty promieniowania EMI (zakłócenia – rys. 6), a jednocześnie bardzo czuły na jakiekolwiek wibracje wywołane przez intruza próbującego wkroczyć na teren chroniony lub nadzorowany. Ułożenie kabla światłowodowego może mieć różne konfiguracje zależne od potrzeb chronionego obiektu.

3. OCHRONA OBWODOWA OBIEKTÓW TRANSPORTOWYCH O ZNACZENIU STRATEGICZNYM

Na rys. 7 przedstawiono obiekt transportowy specjalnego przeznaczenia o znaczeniu strategicznym. Dla prawidłowej ochrony obiektu budowlanego (oznaczony na rysunku jako S) zastosowano bariery mikrofalowe. W tym celu zastosowano cztery zestawy, z których każdy składa się z nadajnika i odbiornika. W pobliżu tego budynku nie ma drzew, a tym samym zmniejsza się prawdopodobieństwo wystąpienia fałszywych alarmów. Cały teren zabezpieczono poprzez zastosowanie kabla sensorycznego, który został umieszczony na ogrodzeniu. Ponieważ całość terenu jest dość duża, a tym samym również długość ogrodzenia jest znaczna, zastosowano podział całego ogrodzenia na poszczególne odcinki. Założono, że będzie ono składało się z sześciu wydzielonych segmentów w skład których będzie wchodził jeden punkt koncentracyjny oraz dwa segmenty kabla sensorycznego. Pozwoli to na zmniejszenie długości pojedynczego odcinka kabla sensorycznego, co przekłada się na precyzyjniejsze wykrycie ewentualnego wtargnięcie na teren rozpatrywanego obiektu transportowego.



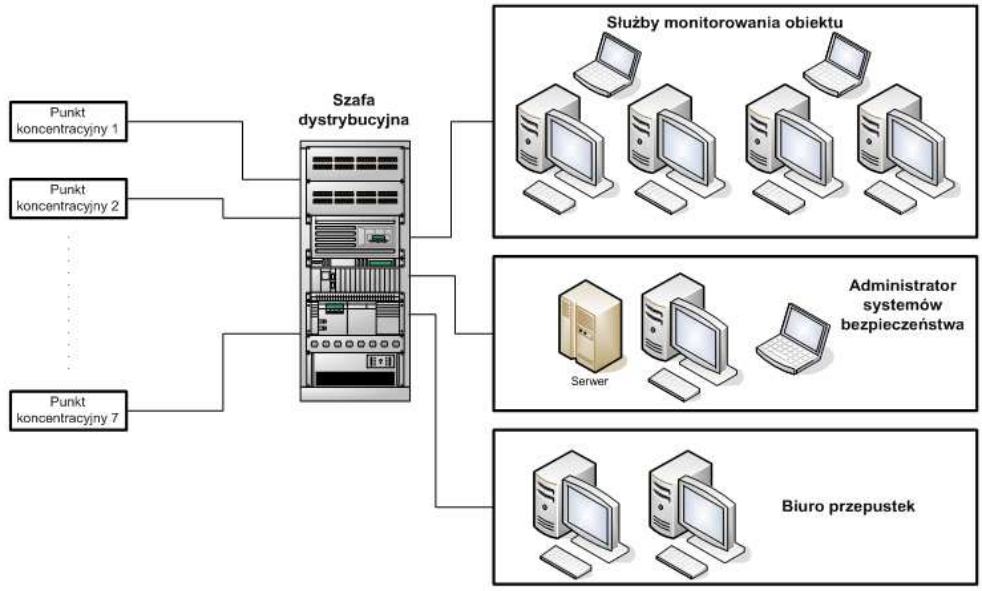
Rys. 7. Obiekt transportowy o znaczeniu strategicznym wraz obwodowym systemem ochrony (aktywne bariery mikrofalowe oraz kable sensoryczne)

Aby zaprojektowany system bezpieczeństwa spełniał prawidłowo swoje cele, niezbędne jest przesłanie informacji z punktów koncentracyjnych (sześciu z kabli sensorycznych i jednego z barier mikrofalowych) do wydzielonych stanowisk:

- służb monitoringu obiektu,
- administratora systemów bezpieczeństwa,
- biura przepustek.

Schemat blokowy połączeń pomiędzy punktami koncentracyjnymi a wymienionymi stanowiskami pokazano na rys. 8. W celu zapewnienia bezpieczeństwa transmisji [1,10] (m.in. przed zakłóceniami elektromagnetycznymi) zastosowano jednomodowe kable

światłowodowe. Oczywiście należy pamiętać, że po stronie nadawczej i odbiorczej łącz światłowodowych należy zastosować konwertery światłowodowe przetwarzające sygnały elektryczne na optyczne (nadajnik) i optyczne na elektryczne (odbiornik) [3].



Rys. 8. Schemat blokowy połączeń pomiędzy punktami koncentracyjnymi a stanowiskami służb bezpieczeństwa

4. WNIOSKI

W artykule dokonano przeglądu metod i sposobów wykorzystywanych współcześnie w elektronicznych systemach obwodowej ochrony obiektów. Zaprezentowano poszczególne rozwiązania z podaniem ich zalet i wad (z uwzględnieniem warunków środowiskowych i wymagań funkcjonalnych stawianych obecnie tego typu systemom). Pozwoliło to na opracowanie koncepcji systemu obwodowej ochrony obiektu transportowego o znaczeniu strategicznym.

Realizując system ochrony obwodowej tego typu obiektów należy uwzględniać szereg czynników, które mają wpływ na dobór urządzeń, metod transmisji sygnałów, a także na realizację stanowiska ochrony, na którym możliwym będzie zarządzanie systemami jak i bezpieczeństwem obiektu. Czynnikami tymi są m.in.: przeznaczenie obiektu, wielkość (rozległość), położenie i odległość od innych obiektów, kubatura budynków znajdujących się na terenie obiektu, zagospodarowaniem terenu wewnątrz obiektu (w tym zalesienie).

5. BIBLIOGRAFIA

[1] Haykin S.: *Systemy telekomunikacyjne. Tom I i II*, Warszawa, WKiŁ 2004.
[2] Hołyst B.: *Terroryzm. Tom 1 i 2*, Warszawa, Wydawnictwo prawnicze LexisNexis 2009.
[3] Horowitz P., Hill W.: *Sztuka elektroniki. Tom I i II*, Warszawa, WKiŁ 2006.

[4] Instrukcje serwisowe systemów i urządzeń firm: DSC, KABE, RISCO, SATEL.
[5] Jankowski G.: *Systemy ochrony obwodowej obiektów o przeznaczeniu specjalnym – koncepcja systemu* (Praca dyplomowa), Warszawa, WSM w Warszawie 2010.
[6] Materiały firmy oraz instrukcje instalatora urządzeń firmy COMPAS.
[7] Materiały informacyjne oraz instrukcje instalatora urządzeń firmy ATLINE.
[8] Materiały producenta systemu Ifter InPro BMS.
[9] Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
[10] Szulc W. Rosiński A.: *Systemy sygnalizacji włamania. Część 3 – Magistrale transmisyjne i metody transmisji danych*, Zabezpieczenia Nr 4(68)/2009, Warszawa, wyd. AAT 2009.