TECHNIKA TRANSPORTU SZYNOWEGO

Joanna ĆWIRKO, Robert ĆWIRKO

ROZWAŻANIA O SYSTEMACH SYGNALIZACJI WŁAMANIA I NAPADU W STACJONARNYCH OBIEKTACH TRANSPORTOWYCH

Streszczenie

Rynek systemów bezpieczeństwa oferuje wiele różnorodnych systemów alarmowych i ich podzespołów. Poprawność projektowania i instalowania systemów alarmowych jest codziennie weryfikowana przez włamywaczy. Celem artykułu jest przedstawienie zabezpieczeń wybranych elementów systemu bezpieczeństwa. Przeprowadzono analizę podstawowych uwarunkowań typów instalacji czujek, mających wpływ na bezpieczeństwo systemu alarmowego. Ostatnią część artykułu poświęcono testom zabezpieczeń czujek PIR i przedstawieniu metod antymaskingu tych czujek.

WSTĘP

Stacjonarne obiekty kolejowe a więc stacje i dworce kolejowe w obecnych czasach wymagają ochrony poprzez instalacje profesjonalnych systemów alarmowych. Jednocześnie są to obiekty o specyficznych cechach i w konsekwencji nie jest łatwo zaprojektować odpowiedni system alarmowy. Dodatkowo są to zwykle miejsca, gdzie dziennie przemieszczają się tysiące anonimowych pasażerów. Systemy ochrony powinny chronić obiekty jednocześnie przed celowym działaniem przestępców, sabotażem i dewastacją przez niezadowolonych pasażerów.

Przy wyborze systemu alarmowego, a zwłaszcza typu centrali alarmowej, przyszły użytkownik zwraca główną uwagę na jego parametry techniczne: liczbę wejść dozorowych do podłączenia czujek, dodatkowe funkcje typu harmonogramy czasowe itp. Producentom systemów central alarmowych zależy, co jest naturalne, na tym by ich sprzedaż była jak największa. Dlatego też próbują zachęcić potencjalnych użytkowników takimi rozwiązaniami jak: coraz łatwiejszymi w obsłudze programami do konfiguracji centrali alarmowej, publikowaniem w Internecie pełnej dokumentacji danego typu centrali, sprzedaży poza systemem firm zajmujących się branżą systemów ochrony itp. Niestety ujemnym skutkiem tych działań jest to, że coraz szersza grupa przestępców ma możliwość praktycznie nauczyć się sposobów unieszkodliwiania tak reklamowanych typów systemów alarmowych.

1. WYBRANE ZAGADNIENIA SKUTECZNOŚCI ZABEZPIECZEŃ SYSTEMÓW SYGNALIZACJI WŁAMANIA I NAPADU

Struktura systemu sygnalizacji włamania i napadu - SWiN (potocznie nazywanego systemu alarmowym) bazuje na module centrali alarmowej do której podłączone są różne rodzaje czujek [1].

Najczęściej wykorzystywane typy czujek to: czujki piroelektryczne (PIR), magnetyczne czujki kontaktronowe i czujki sygnalizujące stłuczenie szyby. Stosuje się też czujki mikrofalowe bazujące na zjawisku Dopplera, czujki reagujące na przerwanie toru podczerwieni lub mikrofal, czujki światłowodowe reagujące na nacisk, czujki ultradźwiękowe, czujki sejsmiczne itp.

Przyjęcie przez centralę sygnału alarmowego z czujki może powodować różnorodne działania, na przykład: uruchomienie sygnalizatora akustycznego z opcją sygnalizacji optycznej, uruchomienie sygnalizatora akustycznego z jednoczesnym wysłaniem odpowiedniego komunikatu do stacji monitoringu (ACO), wysłanie komunikatu do centrum monitoringu bez włączania sygnalizatora akustycznego, tzw. cichy alarm, wykorzystanie wyjść funkcyjnych centrali do opcjonalnego uruchomienia oświetlenia terenu itp.

Ewentualny przestępca ma kilka możliwości unieszkodliwienia systemu alarmowego:

- wyłączenie systemu alarmowego z czuwania;
- uszkodzenie toru transmisji alarmu lub sygnalizatorów;
- uszkodzenie linii komunikacyjnych (dozorowych) między czujkami a centralą;
- uszkodzenie lub neutralizacja czujek.

Stacjonarne obiekty transportowe, czyli stacje i dworce kolejowe, za wyjątkiem największych stacji np. Poznań, formalnie, zgodnie z normą dotyczącą systemów alarmowych [2] z 2009 roku, należy zaliczyć do obiektów klasy 1. Norma ta dzieli obiekty na klasy ze względu „umiejętności włamywaczy". Z drugiej jednak strony, uwzględniając specyfikę stacji kolejowych, w tym duże zakłócenia elektromagnetyczne, należy je zaliczyć do klasy 2. Przypisanie obiektu do wyższej klasy powoduje konieczność stosowania elementów i rozwiązań systemu alarmowego o większym stopniu zabezpieczenia przed intruzami.

1.1. Wyłączenie systemu alarmowego lub uszkodzenie torów transmisji

Włamywacz może próbować wyłączyć system alarmowy z dozoru (czuwania) na kilka sposobów:

- wyłączenie systemu alarmowego po siłowym zmuszeniu użytkownika do wprowadzenia do manipulatora kodu rozbrojenia (wyłączenia z dozoru);
- podjęcie działań psychologicznych, na skutek których użytkownik wyłączy bez przymusu system alarmowy;
- zdobycie kodu rozbrojenia centrali alarmowego;

Metody te są związane są na ogół z niezamierzonym udziałem użytkownika systemu alarmowego.

Dla obiektów o małym zagrożeniu wystarczają sygnalizatory dźwiękowe lub dźwiękowo-optyczne. Obiekty o wyższym stopniu ryzyka szkód wymagają również zgodnie z obowiązującymi normami zastosowania jednego lub dwóch niezależnych torów transmisji do stacji monitoringu (ACO).

Tor transmisji może być realizowany jako połączenie przewodowe komutowane (linia telefoniczna) lub bezprzewodowe – radiowe lub sieć GSM/GPRS.

Uszkodzenie toru transmisji do stacji monitoringu (ACO) można zrealizować przez:

- odcięcie lub zablokowanie linii telefonicznej od centrali alarmowej;
- zagłuszenie radiowej lub GSM/GPRS transmisji informacji alarmowej z centrali alarmowej.

Jeżeli centrala alarmowa została skonfigurowana tak, aby sygnały alarmowe i informacyjne były przekazywane z centrali alarmowej do stacji monitoringu za pośrednictwem komutowanej linii telefonicznej, to modem centrali sprawdza okresowo (co kilka minut) stan linii telefonicznej czy nie nastąpiło jej uszkodzenie, na przykład na skutek przecięcia.

Intruz chcąc zagłuszyć transmisję radiową ma do wyboru następujące możliwości: włączyć urządzenie zagłuszające przed wejściem do chronionego obiektu lub prowadzić nasłuch, kiedy interfejs radiowy zaczynie wybierać numer ACO i dopiero po tym włączyć zagłuszanie. Ten drugi sposób zmniejsza prawdopodobieństwo wykrycia włączenia urządzenia zagłuszającego przez przestępcę. Na rysunku 1a przedstawiono wykrywacz telefonów komórkowych DS-200. Wykrywacz może współpracować z urządzeniem zagłuszającym, na przykład GSM GS-107F (rys. 1b) [3].

a) *b)*

Rys. 1. Wykrywacz transmisji komórkowej DS-200 *(a)* i urządzenie zagłuszające GSM GS-107F *(b)*

W momencie wystąpienia jakiegokolwiek sygnału transmisji radiowej, na przykład rozpoczęcia przez moduł GSM centrali alarmowej wybierania numeru stacji monitoringu, urządzenie zagłuszające zostanie aktywowane przez DS-200 w czasie nie dłuższym niż 20 ms. Urządzenie GS-107F zagłusza systemy łączności cyfrowe bazujące na standardach : CDMA, GSM, DCS i 3G. Maksymalna moc wyjściowa urządzenia wynosi 11 W, co pozwala na zagłuszenie nadajnika radiowego centrali alarmowej w promieniu 10 – 40 metrów (w zależności od ustawienia anten i warunków terenowych). Urządzenie zagłuszające ma możliwość regulacji mocy zagłuszania osobno na każde pasmo.

O ile z klasy ochrony obiektu nie wynika konieczność istnienia dwóch niezależnych torów transmisji stacji monitoringu, użytkownik systemu alarmowego ma zwykle problem z podjęciem decyzji co do ilości torów transmisyjnych.

W przypadku obiektów jak stacje kolejowe należy sugerować wybór dwóch nieależnych kanałów transmisji, na przykład telefonicznej sieci komutowanej i telefonii GSM gdyż zwiększa to odporność systemu ochrony na ewentualne próby sabotażu.

1.2. Niezawodność linii komunikacyjnych miedzy czujką a centralą

Linie komunikacyjne miedzy czujką a centralą alarmową mogą być realizowane jako przewodowe lub bezprzewodowe. Komunikacja bezprzewodowa ma swoja ogromna zaletę – łatwość montażu, ale znacznie wyższą cenę SSWiN.

Dodatkowo, tereny kolejowe charakteryzują się znacznymi zakłóceniami elektromagnetycznymi, co może mieć istotny wpływ na niezawodność komunikacji między czujkami a centralą.

Dlatego, w systemach SWiN w takich obiektach dobrym rozwiązaniem jest stosowanie klasycznych przewodowych linii dozorowych do centrali. W przypadku linii przewodowych odporność na próby uszkodzenia linii zależy od sposobu podłączenia czujek. Sposób podłączenia czujki do centrali alarmowej zależy od zastosowanych w czujce rozwiązań konstrukcyjnych mających za zadanie przekazanie informacji o zmianie jej stanu z czuwania w stan alarmu. Najczęściej następuje to po zmianie wysterowania przekaźnika na wyjściu czujki, który przełącza swoje zestyki, na przykład ze zwarcia (NC) w stanie czuwania, do rozwarcia w stanie wykrycia alarmu. Dla takiego rozwiązania układowego, do każdego wejścia dozorowego centrali alarmowej podłącza się jedną czujkę. Zestyk przekaźnika czujki można podłączyć w sposób bezpośredni do wejścia linii dozorowej centrali alarmowej, ale preferowane jest jego podłączenie za pośrednictwem rezystorów parametryzujących (EOL lub 2EOL), gdyż pozwala to wykryć dodatkowo sytuacje związane z próbą przecięcia linii dozorowej lub próbą zwarciowego obejścia zestyku przekaźnika czujki.

Centrala alarmowa monitoruje linie dozorowe odpowiednio, pod względem przerwy, przerwy i zwarcia a nawet względem wszystkich zakłóceń przeszkadzających w transmisji sygnału z czujki do centrali. Zakres monitorowania linii dozorowych zależy od klasy obiektu chronionego, ale jest możliwy tylko przy podłączeniu czujek typu EOL lub 2EOL

Niektóre centrale alarmowe posiadają wydzieloną magistralę dwuprzewodową do której można dołączyć jednocześnie do kilkudziesięciu czujek adresowalnych. Każda z tych czujek posiada nadany przez producenta niepowtarzalny adres, za pomocą którego jest ona identyfikowana po przyłączeniu do magistrali. Zaletą tego rozwiązania jest możliwość dołączania kolejnych czujek bez prowadzenia dodatkowego okablowania lub zwiększania linii dozorowych za pomocą dodatkowych modułów. Jednakże w przypadku uszkodzenia toru transmisyjnego takiej magistrali dwuprzewodowej, centrala alarmowa przestaje widzieć wszystkie dołączone do tej magistrali czujki.

Dla typowego rozwiązania, z użyciem klasycznych linii dozorowych, uszkodzenie linii transmisyjnej łączącej czujkę z wejściem dozorowym centrali eliminuje tylko tą czujkę i po uaktywnieniu przez użytkownika funkcji „bypass" ta linia dozorowa zostaje wyłączona elektrycznie ze struktury centrali i nie zakłóca działania pozostałych czujek.

Ponieważ tory transmisyjne linii dozorowych są narażone na oddziaływanie różnorodnych zakłóceń zewnętrznych, na przykład wyładowań atmosferycznych, zakłóceń od linii energetycznych, telefonii komutowanej itp., ustala się dla sygnału alarmowego z czujki pewien minimalny czas trwania, poniżej którego sygnał jest interpretowany jako zakłócenie. W większości central alarmowych jest to 350-500 ms.

Wyjątkiem są wejścia linii dozorowych służących do podłączenia czujek zbicia szyby. Dla części typów takich czujek, dokonywana jest w centrali alarmowej analiza widmowa sygnałów przychodzących w czasie tłuczenia szyby i na podstawie tej analizy podejmowana jest decyzja, czy należy uruchomić procedurę alarmu, czy też traktować przychodzące sygnały jako zakłócenia. Jednakże dla takiej analizy widmowej wejście linii dozorowej musi być ustawione dla przyjmowanie sygnałów o krótszych czasach trwania, na przykład 10-15 ms, niż z pozostałych linii dozorowych, celem przyjęcia odpowiedniej liczby próbek.

1.3 Możliwości unieszkodliwienia i zabezpieczenia czujek PIR

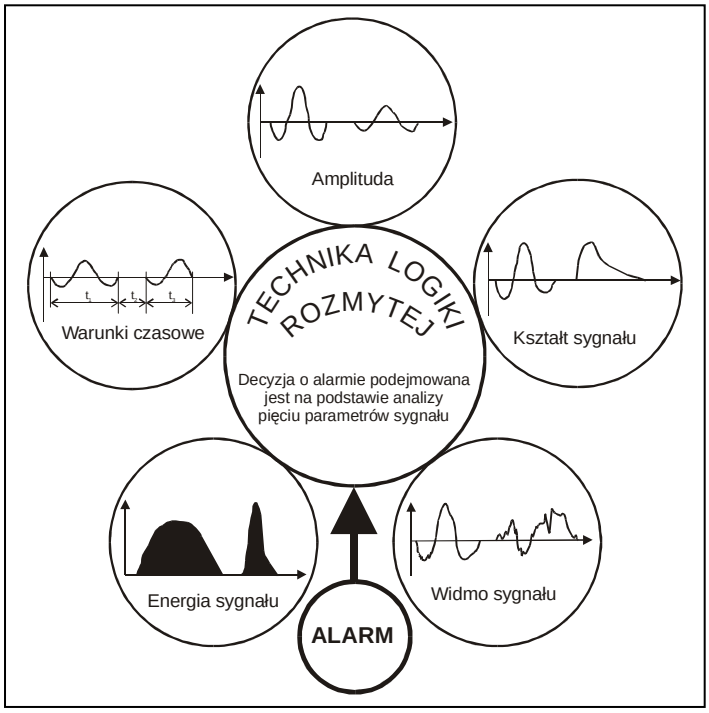
Pasywne czujki podczerwieni PIR (*ang. Passive InfraRed*) są powszechnie stosowane w różnorodnych systemach ochrony oraz elementach automatyki. Wykrywają przemieszczanie się w obszarze objętym ich zasięgiem obiektów, których temperatura różni się od temperatury otoczenia przez analizę szybkości zmian promieniowania podczerwonego. Detektor piroelektryczny czujki jest czujnikiem wykrywającym wielkość zmian temperatury a nie jej wartość. Średni prąd detektora jest proporcjonalny do szybkości zmian temperatury [4]. W

praktyce modulację promieniowania podczerwonego, docierającego do czujki od intruza o stałej temperaturze różnej od tła, uzyskuje się przy użyciu odpowiedniego układu optycznego. W układzie optycznym następuje podział pola widzenia detektora na kilka lub kilkanaście fragmentów – na strefy aktywne i pasywne.

W większości czujek PIR stosuje się wiązkowy podział przestrzeni realizowany przy użyciu tanich soczewek Fresnela wykonanych z plastiku. W droższych typach czujek PIR z optyką zwierciadlaną możliwy jest kurtynowy podział przestrzeni. Dla obydwu podziałów przestrzeni wiązkowej i kurtynowej koniecznym warunkiem wykrycia obiektu o innej temperaturze niż tło jest jego przemieszczanie się pomiędzy strefami pasywnymi i aktywnymi. Na rynku jest dostępna duża różnorodność czujek PIR - w zależności od „pola widzenia" są czujki szerokokątne, dalekiego zasięgu czy sufitowe. Przykładowo w czujce typu Extravision firmy Elektron został zastosowany nietypowy układ optyczny. Soczewka ma kształt sferyczny i jest podzielona na 3 części, z których każda ma inną charakterystykę detekcji widma termicznego: szerokokątną, dalekiego zasięgu i kurtynową. Aby zmienić rodzaj soczewki, w zależności od potrzeby, wystarczy obrócić ją o kąt 120^{o}.

Do obróbki sygnałów z wyjścia detektora piroelektrycznego stosuje się specjalnie skonstruowane układy scalone ASIC (rys. 2). Układy te zawierają między innymi wzmacniacz sygnału, procesor sygnału, komparator, układ logiczny, układ wyjściowy oraz układ diagnostyczny. Cyfrowa obróbka polega na porównaniu charakterystyki sygnału, a więc amplitudy, kształtu i długości trwania impulsu ze wzorcami impulsów zapisanymi w pamięci, których może być nawet kilka tysięcy.

W wielu czujkach PIR najwyższej klasy do analizy sygnału z detektora jest stosowana logika rozmyta Decyzja o alarmie jest podejmowana na podstawie analizy pięciu parametrów sygnału: szybkości zmian, prawidłowości kształtu, amplitudy, energii i widma sygnału. Oczywiście im więcej parametrów sygnału podlega analizie, tym mniej fałszywych alarmów i jednocześnie większa pewność wykrycia intruza.



Rys. 2. Wielotorowa obróbka cyfrowa sygnału z detektora czujki PIR w układzie ASIC

Rozmaitość typów czujek PIR na rynku jest bardzo duża. Rozpiętość cen jest również duża - w skali od 1 do 10. Liczbowo są to czujki, które dominują w każdym systemie SWiN – w

związku z tym decydują jakości i niezawodności a także o końcowej cenie całego systemu ochrony.

1.3.1. Badania czujek PIR

Człowiek emituje promieniowanie podczerwone z zakresu 8-10 μm. Teoretycznie więc, jeżeli ciało człowieka zostanie osłonięte materiałem izolującym termicznie, to stanie się on niewidoczny dla czujki PIR.

Dla określenia jaki materiał izolujący termicznie pozwala najlepiej stłumić promieniowanie podczerwone emitowane przez człowieka przeprowadzono badania, polegające na wykonaniu szeregu zdjęć przy użyciu kamery termowizyjnej.

Na rysunku 3 przedstawiono zdjęcia człowieka ubranego w strażacki skafander ochronny. Pasek po prawej stronie obrazuje odcień szarości odpowiadający danej temperaturze na termogramie.

Ochronny skafander strażacki jest wykonany z materiału odbijającego promieniowanie cieplne. Na termogramie widoczne są niewielkie różnice pomiędzy temperaturą tła a człowiekiem ubranym w ten skafander. Jeżeli człowiek tak ubrany wejdzie do pomieszczenia chronionego przez czujkę PIR to jej poziom detekcyjności może się okazać niewystarczający do wywołania alarmu.

Rys. 3. Człowiek ubrany w strażacki skafander ochronny - widok normalny i w podczerwieni [5]

Badaniom zostały poddane trzy czujki różnych producentów o podobnym zasięgu znamionowym około 9 metrów:

- Enforce Super (montaż na wysokości 2 m),
- Magnum True Quard (montaż na wysokości 2 m),
- Equinox AM (montaż na wysokości 2,4 m).

W tabeli 1 przedstawiono przykładowe wyniki pomiarów dla czujki Magnum True Quard. Zdolność wykrywania czujki PIR zależy od kierunku ruchu obiektu wykrywanego. Jest ona mniejsza dla ruchu poosiowego. Szukając słabych punktów systemu alarmowego należy sprawdzić możliwość podejścia do czujki PIR przez intruza poruszającego się w osi czujki.

Tab. 1. Wpływ ubioru na działanie czujki Magnum True Quad

Odległość [m]	Rodzaj zastosowanego ubioru			
	Normalny	Strój strażacki	Normalny	Strój strażacki
1	✓	✓	✓	✓
2	✓	✓	✓	✓
3	✓	✓	✓	✓
4	✓	✓	✓	✓
5	✓	×	✓	×
6	✓	×	✓	×
7	×	×	×	×
8	×	×	×	×
9	×	×	×	×
10	×	×	×	×
	Ruch wolny 0.1 m/s		Ruch normalny 1 m/s	

× - czujka nie wykryła ruchu
✓ - czujka wykryła ruch

Badanie, którego wynik zamieszczono w tabeli 2 przeprowadzono poruszając się w kierunku „do czujki" z prędkością 0,1 m/s. Próbę powtarzano 10-krotnie i 10-krotne poosiowe podejście w ochronnym stroju strażackim nie zostało zasygnalizowane przez czujkę Magnum True Quard.

Tab. 2. Odporność czujek na ruch poosiowy

Czujka	Enforcer Super		Magnum True Quad		Equinox AM	
Rodzaj stroju	Normalny	Strój strażacki	Normalny	Strój strażacki	Normalny	Strój strażacki
Odległość [m]	5	3	2.5	Nie wykryty	8	5

1.3.2 Maskowanie czujek PIR

Niejednokrotnie włamanie do obiektu jest poprzedzone wielotygodniowymi przygotowaniami. Wejście do obiektu pod różnymi pozorami ma na celu zidentyfikowanie systemu alarmowego (czy jest on zainstalowany, jaki jest typ sytemu, rodzaje czujek zastosowanych w obiekcie) lub też unieszkodliwienie zainstalowanego systemu. Zostawiony „bez opieki", przestępca może w ciągu 3-5 sekund przekręcić czujkę w kierunku ściany, co spowoduje powstanie „strefy martwej" czyli obszaru nie objętego dozorem, lub zwyczajnie zakleić ją kawałkiem taśmy, czyli przeprowadzić tzw. maskowanie czujki PIR. Maskowanie czujek ruchu jest jedną z często wykorzystywaną przez przestępców metodą mająca na celu neutralizację systemu alarmowego.

W celu określenia wpływu maskowania na zasięg rzeczywisty czujek przeprowadzone zostały badania polegające na wyznaczeniu zasięgu rzeczywistego dla czujek przysłoniętych trzema rodzajami materiałów:

- A – maskowanie dwiema warstwami biurowej taśmy bezbarwnej;

- B – maskowanie przezroczystą taśmą pakową podklejoną białym papierem;
- C - maskowanie lakierem do włosów.

Soczewki w większości czujek mają kolor mlecznobiały, więc wykonanie maskowania z materiałów A i B nie jest widoczne. Także naniesiona cienka warstwa lakieru do włosów po wyschnięciu staje się niewidoczna. Jako materiały maskujące wybrano materiały powszechnie dostępne, których założenie na czujkę nie zostanie natychmiast zauważone.

Testy przeprowadzone zostały na trzech czujkach ruchu firmy Pyronix: Enforcer Super (czujka PIR), Magnum True Quad (czujka PIR), oraz Equinox AM (czujka dualna PIR+MW z wbudowaną funkcją antymaskingu).

Metodyka pomiarów była identyczna z wykorzystywaną podczas pomiarów weryfikacyjnych badań termograficznych opisanych wcześniej. Znamionowy zasięg badanych czujek wynosił 8 metrów.

Jako przykładowy przedstawiono w tabeli 3 wpływ zastosowania maskowania na zasięg rzeczywisty czujki Magnum True Quard. Jak widać, najbardziej efektywnym materiałem była przezroczysta taśma pakowa podklejona białym papierem. Lakier do włosów nie tłumi promieniowania podczerwonego.

Tab. 3. Wpływ zastosowanego maskowania na zasięg rzeczywisty czujki Magnum True Quad

Odległość od czujki [m]	Szybkość ruchu poprzecznego							
	0.1 m/s				1 m/s			
1	✓	✓	×	✓	✓	✓	×	✓
2	✓	✓	×	✓	✓	✓	×	✓
3	✓	✓	×	✓	✓	✓	×	✓
4	✓	✓	×	✓	✓	✓	×	✓
5	✓	×	×	✓	✓	×	×	✓
6	✓	×	×	✓	✓	×	×	✓
7	✓	×	×	✓	✓	×	×	✓
8	×	×	×	×	×	×	×	×
9	×	×	×	×	×	×	×	×
10	×	×	×	×	×	×	×	×
		A	B	C		A	B	C
		Maskowanie				Maskowanie		

× - czujka nie wykryła ruchu

✓ - czujka wykryła ruch

Aby uniknąć konsekwencji tego typu zdarzeń, powodowanych umyślnie przez przestępców lub nieumyślnie przez użytkowników systemu alarmowego, producenci czujek PIR wprowadzili dodatkową funkcję, a mianowicie *antymasking.*

Funkcja ta pozwala na monitorowanie stanu przysłonięcia czujki. Zwykle czujka z antymaskingiem posiada dodatkowe wyjście, na którym sygnalizowana jest próba przysłonięcia, nawet podczas wyłączenia stanu czuwania systemu.

Według norm, w czujki PIR stosowane w systemach alarmowych wyższych klas, powinny mieć funkcje wykrywania znacznej redukcji swojego zasięgu znamionowego.

Antymasking w czujkach PIR może być realizowany na wiele sposobów. Na uwagę zasługują trzy systemy opracowane przez Centrum Badawczo-Rozwojowe firmy Bosch [6]. Pierwszy z nich nosi nazwę „*Begunce-Beck*" i polega na wytworzeniu wokół czujki pewnego rodzaju

„bańki" promieniowania podczerwonego rozciągającej się na około 30 cm. Czujka jest wyposażona w dwie fotodiody, które reagują na zwiększenie mocy promieniowania do nich docierającego. Podczas normalnej pracy promieniowanie „bańki" IR nie dociera do fotodiod, przysłonięcie czujki powoduje odbijanie części promieniowania od przeszkody i oświetlenie fotodiod. Drugi system wykrywania maskowania czujki nosi nazwę „*Retro Reflektor*" i opiera się na technologii „wielu pryzmatów". Czujka posiada wbudowany emiter podczerwieni. Promieniowanie emitowane jest na strukturę wielopryzmatową, która całkowicie odbija je w kierunku wbudowanej fotodiody podczerwieni. Zamalowanie czujki powoduje, iż pryzmaty tracą swoje właściwości. Moc promieniowania docierającego do fotodiody gwałtownie maleje, co powoduje wyzwolenie sygnału alarmowego. Trzeci system „*Trough the Lents*" wykrywa próby przysłonięcia soczewki czujki PIR. Zasada tego antymaskingu jest następująca. Czujka emituje promieniowanie podczerwone, które odbija się od dwóch pryzmatów umieszczonych w dolnych rogach czujki i trafia na soczewkę Fresnela. Zamaskowanie soczewki powoduje spadek sygnału docierającego do fotodiody IR znajdującej się za soczewką i wywołuje sygnał alarmu.

PODSUMOWANIE

Artykuł przedstawia rozważania dotyczące uwarunkowań technicznych stosowania systemów sygnalizacji i włamania na stacjach i dworcach kolejowych. W artykule omówiono strukturę typowego systemu alarmowego zawierającego różnorodne czujki. Przeprowadzono analizę podstawowych uwarunkowań typów instalacji czujek, mających wpływ na bezpieczeństwo systemu alarmowego. Drugą część artykułu poświęcono testom zabezpieczeń czujek ruchu PIR, które są najczęściej stosowanymi czujkami w systemach alarmowych. Przedstawiono również metody antymaskingu tych czujek.

W artykule zwrócono uwagę na podstawowe problemy związane z wyborem właściwego systemu alarmowego dla specyficznych obiektów jakimi są stacje i dworce kolejowe.

OF CONSIDERING THE BURGLARY AND THE ASSAULT ABOUT NOTIFICATION SYSTEMS IN STATIONARY TRANSPORT OBJECTS

Abstract

The market of securities is offering many alarm systems and their components. Validity of designing and installation of alarm systems is examine by buglers, every day. The aim of this article is showing protection systems of chosen compound security systems. The paper presents analysis of influence of kind of installation sensors on validity of alarm system. The last part of article contain some test of protection on PIR sensor and describe on antymasking system of PIR sensor.

BIBLIOGRAFIA

1. Red. Wójcik A.: *Mechaniczne i elektroniczne systemy zabezpieczeń*. Verlag Dashofer 2009.
2. *Normy z grupy PN-EN 5013 Systemy alarmowe* – Systemy sygnalizacji włamania.
3. Materiały firmy Euro-Soft. *Strona internetowa http://euro-soft.pl.*
4. Bielecki Z., Rogalski A.: *Detekcja sygnałów optycznych*. Wydawnictwo Naukowo-Techniczne, 2001, ISBN 83-204-2654-5.

5. Bućkowski R.: *Analiza skuteczności zabezpieczeń systemów ochrony przed nieuprawnionym dostępem.* Praca dyplomowa. Wojskowa Akademia Techniczna.
6. Kostecki K.: *Inteligentne czujki z serii Professional z wielopunktowym antymaskingiem*. Zabezpieczenia 2/2008.

Autorzy:
dr inż. Joanna Ćwirko – Wojskowa Akademia Techniczna ISE WEL, Warszawa
dr inż. Robert Ćwirko – Wojskowa Akademia Techniczna ISE WEL, Warszawa