AKADEMIA
OBRONY NARODOWEJ

Do użytku służbowego

Egz. Nr .....

Płk dr inż. Eugeniusz PIEDZIUK

SYSTEMY ALARMOWE SYGNALIZACJI ZAGROŻEŃ

WARSZAWA 1998

AKADEMIA OBRONY NARODOWEJ

ZAKŁAD ZARZĄDZANIA SYSTEMAMI INFORMACYJNYMI

Do użytku służbowego

Egz. nr .....

Płk dr inż. Eugeniusz PIEDZIUK

SYSTEMY ALARMOWE SYGNALIZACJI ZAGROŻEŃ

WARSZAWA MARZEC 1998

Praca została wykonana na podstawie opracowań teoretycznych Biblioteki Głównej AON, dzienników ustaw oraz dokumentacji technicznej firm:

- ATM S.A.;
- DGT Sp. z o.o.;
- Efecta Sp. z o.o.;
- Motorola;
- Opto Sp. z o.o.;
- Sezam Sp. z o.o.

SPIS TREŚCI

SPIS RYSUNKÓW

WSTĘP

W ostatnich latach obserwujemy w Polsce systematyczny wzrost przestępczości i wykroczeń różnego typu. Charakteryzują się one się one takimi cechami, jak:

- **profesjonalizacja przestępczości** (rozpracowywanie sytuacji przed dokonaniem przestępstwa, planowanie jego realizacji, prowadzenie przygotowań organizacyjnych i technicznych, wykorzystywanie nowoczesnych środków technicznych i łączności, przydzielanie określonych ról i funkcji w grupie przestępczej),
- **stosowanie broni palnej, materiałów wybuchowych i innych przedmiotów niebezpiecznych**,
- **umiędzynarodowienie** (przemyt samochodów i narkotyków),
- **agresja**,
- **okrucieństwo**.

Dynamiczny wzrost przestępczości dotyczy nie tylko obywateli, ale także w wysokim stopniu stanowi zagrożenie dla obszarów, obiektów jak i urządzeń obsługujących jednostki organizacyjne oraz centralne instytucje funkcjonujące na potrzeby obronności i bezpieczeństwa kraju. Pojawiające się zagrożenia skierowane między innymi przeciwko tym instytucjom budzą szczególny niepokój ze względu na kluczowe znaczenie tych organów dla stabilnego funkcjonowania państwa.

W strukturach administracyjnego zarządzania i kierowania bezpieczeństwem państwa jednostki wojskowe jak i odpowiednie struktury ministerstwa obrony narodowej, resortu spraw wewnętrznych i administracji oraz obrony cywilnej stanowią podstawową formę organizacyjną systemu obronnego kraju. Ich organizacja, różnorodność funkcjonowania, wzajemne relacje oraz ilość, utrudnia stworzenie wzorcowego modelu ochrony przed różnego typu zagrożeniami. Należy nadmienić, że zagrożenia przestępcze szczególnie będą się wzmagać w czasie klęsk ekologicznych, katastrof i wojny.

Analizując rozwój wielu dziedzin wiedzy z zakresu elektroniki, telekomunikacji, informatyki można stwierdzić, że w największym stopniu narażone będą nośniki informacji, trakty i podzespoły przesyłowe, urządzenia końcowe wraz z ich obiektami.

Istnieje więc konieczność ochrony obiektów i mienia przed różnorodnymi zagrożeniami. Urządzenia alarmowe stają się coraz bardziej powszechnymi i skutecznymi

środkami neutralizacji zagrożeń przestępczych i cywilizacyjnych tak w środowisku cywilnym, jak i w strukturach zarządzających krajem.

Dla swej skuteczności systemy te powinny stanowić jeden ze środków neutralizacji zagrożeń , na które składają się :

- rozwiązania architektoniczno - budowlane,
- zabezpieczenia mechaniczne (np. zamki, blokady, zapory),
- urządzenia sygnalizacyjne i systemy wspomagające (np. nadzór TV, kontrola dostępu),
- rozwiązania organizacyjne (np. plany ochrony, procedury reakcji na sygnały alarmowe jak i zagrożenia).

Doskonalenie środków neutralizacji zagrożeń musi być procesem ciągłym oraz kierowanym przez odpowiedzialnych pracowników i nadzorowanym przez ich przełożonych. Tylko w ten sposób można wytrącić inicjatywę sprawcom przestępstw działającym w sposób profesjonalny.

Zapewnienie bezpieczeństwa zawsze wiąże się z dużymi nakładami finansowymi. Jak uczy doświadczenie są one zdecydowanie mniejsze niż te, które są ponoszone na naprawianie różnorakich szkód wynikłych z przestępstwa.

1. OCHRONA OBIEKTÓW I MIENIA

Ogólnie bezpieczeństwo osób i mienia, rozumiane jest jako stan niezagrożenia, spokoju i pewności. Uzależnione jest ono od siły oddziaływania następujących czynników:

- poziomu zagrożenia dóbr prawnie chronionych, które może powstać w wyniku bezprawnego działania innego człowieka (przestępstwa, wykroczenia, czynu niedozwolonego) lub stanowić skutek tzw. zjawisk losowych,
- skuteczności zabezpieczenia technicznego i ochrony fizycznej przed zagrożeniami.

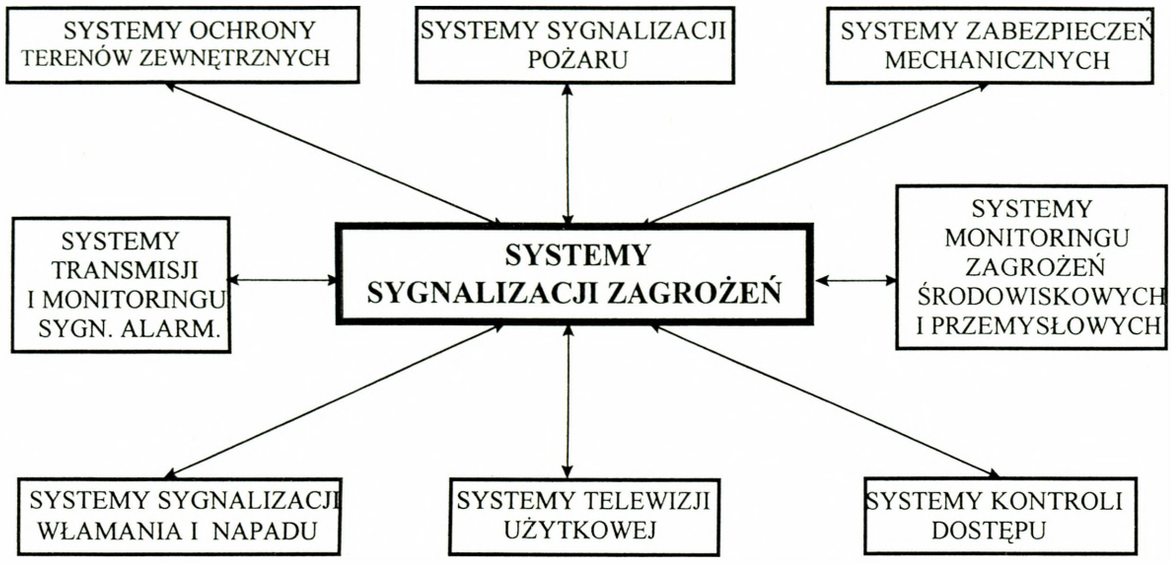
1.1. Pojęcia podstawowe

Na bazie szybkiego rozwoju elektroniki rozwinęła się nowa dziedzina jej zastosowań wyspecjalizowana do ochrony mienia, zdrowia i życia ludzkiego przy pomocy elektronicznych systemów alarmowych sygnalizujących stany zagrożeń.

Rozróżniamy następujące grupy elektronicznych systemów alarmowych:

1. Systemy sygnalizacji pożaru.
2. Systemy alarmowe sygnalizacji włamania, kradzieży i napadu oraz sterowania urządzeniami wykonawczymi.
3. Systemy kontroli (sterowania) dostępu.
4. Systemy telewizji użytkowej (przemysłowej) i nadzoru wideo.

- Systemy monitoringu i transmisji sygnałów alarmu.
- Systemy ochrony zewnętrznej (terenów).



Rys. 1. Rodzaje systemów sygnalizacji zagrożeń

Systemy alarmowe dzieloną się na cztery klasy od SA1 do SA4 według ich własności jakościowych i zdolności do ochrony obiektów w warunkach oddziaływania czynników zewnętrznych.

Podział systemów na klasy uwzględnia:

- klasę zagrożenia obiektu (Z4, Z3, Z2, Z1)[1]
- cechy czujek włamaniowych,
- kontrolę linii dozorowych,
- odporność na oddziaływanie środowiskowych zakłóceń elektromagnetycznych,
- środki transmisji sygnałów alarmowych do miejsc nadzoru,
- ochronę przed dostępem osób niepowołanych,
- kontrolę sprawności (działania) systemu,
- odporność na warunki klimatyczne i środowiskowe,

Klasę urządzenia alarmowego określa się według zasady: poziomu jakości i funkcjonalności tego urządzenia w odniesieniu do odpowiedniej klasy systemu sygnalizacji zagrożeń, w taki sposób, aby dane urządzenie w pełni zabezpieczało wymagania tej klasy systemu.

Klasy urządzeń alarmowych:

[1] Od Z4 do Z1 - obiekty od najwyższej do najniższej kategorii zagrożeń.

A - popularna,

B - standardowe,

C - profesjonalna,

S - specjalna.

Rozróżniamy następujące klasy systemów:

Systemy klasy SA1 - zabezpieczenie obiektów o małym ryzyku szkód oraz pomieszczeń mieszkalnych i gospodarczych oddalonych od urządzeń elektrycznych większej mocy /oddzielone są, i prowadzone w odpowiednich odległości przewody energetyczne i alarmowe/ z urządzeniami typowymi dla gospodarstw domowych /chłodziarki, pralka, sprzęt audiowizualny/, o warunkach klimatycznych typowych dla mieszkań o różnych porach roku.

Systemy klasy SA2 - zabezpieczenie obiektów o średnim ryzyku szkód oraz innych obiektów, w których pracują, urządzenia elektryczne większej mocy /np. winda, hydrofor, lada chłodnicza, lżejsze maszyny produkcyjne itp./ lub pomieszczenia znajdujące się w pobliżu takich urządzeń /gdzie brak separacji między obwodami o różnych poziomach sygnałów i różnych poziomach zakłóceń/.

Systemy klasy SA3 - zabezpieczenie obiektów o dużym ryzyku szkód oraz innych obiektów, w których pracują ciężkie maszyny produkcyjne wytwarzające drgania i wibracje, urządzenia elektryczne dużych mocy lub o komutacji stykowej (brak jest separacji między obwodami zasilania i sygnalizacyjno-sterującymi w wyniku stosowania wspólnych kabli o różnych poziomach sygnałów i zakłóceń) a także obiektów, w których dopuszcza się wyłącznie ogrzewania w dni wolne od pracy.

Systemy klasy SA4 - zabezpieczenia obiektów o bardzo dużym ryzyku szkód, bądź w których występują nietypowe /przynajmniej w jednym czynniku warunki środowiskowe np. bardzo niska lub bardzo wysoka temperatura lub szczególne zakłócenia /np. silne pole elektromagnetyczne/

Ogólna zasada mówi, że nie wolno stosować urządzeń niższej klasy do systemów zakwalifikowanych do wyższej klasy np. do systemu klasy SA2 można stosować urządzenia klasy B i C, natomiast dla systemów klasy SA3 nie można stosować urządzeń klasy A lub B.

Lp.	KATEGORIE ZAGROŻEŃ OBIEKTÓW	KLASY URZĄDZEŃ	KLASY SYSTEMÓW	UWAGI
1.	Z1	A, B, C, S	SA1, SA2, SA3, SA4	zabezpieczenie obiektów o małym ryzyku szkód
2.	Z2	B, C, S	SA2, SA3, SA4	zabezpieczenie obiektów o średnim ryzyku szkód
3.	Z3	C, S	SA3, SA4	zabezpieczenie obiektów o dużym ryzyku szkód
4.	Z4	S	SA4	zabezpieczenie obiektów o bardzo dużym ryzyku szkód

Tab. 1. Kategorie zagrożeń obiektów i odpowiadające im klasy urządzeń i systemów sygnalizacji zagrożeń

Przykład:

Zastosowane rozwiązania w systemach alarmowych zaliczone wstępnie do kategorii zagrożenia np. Z4. Zatem w systemie alarmowym należy zastosować urządzenia klasy profesjonalnej S. W związku z powyższym ochrona obiektów powinna odpowiadać systemowi klasy SA4.

1.2. Elementy systemu sygnalizacji zagrożeń

System sygnalizacji zagrożeń (alarmowy) można podzielić na następujące części składowe:

1) centrala- urządzenie lub zespół urządzeń służące do przyjmowania, przetwarzania sygnału oraz sterowania informacjami systemu alarmowego.
2) czujka- urządzenie przeznaczone do wytwarzania stanu alarmowania w odpowiedzi na wykrycie nienormalnych warunków, wskazujących na wystąpienie niebezpieczeństwa.
3) zasilacz- urządzenie, które przekształca, gromadzi lub wydziela energię elektryczną na potrzeby systemu alarmowego, występujące jako oddzielne urządzenie lub jako część integralna urządzenia sterującego i wskazującego. Zasilacz dostarcza energię do systemu w warunkach normalnych, przy stanie alarmowania i przy zakłóceniach.

4) sprzęt sygnalizacji optycznej i/lub akustycznej- urządzenia, których zadaniem jest poprzez sygnały optyczne i/lub akustyczne poinformować służby ochrony lub innych użytkowników o grożącym niebezpieczeństwie.
5) urządzenia uruchamiane przez centralę np. oświetlenie bezpieczeństwa, wentylatory itd.
6) urządzenia wejściowe programowane- urządzenia służące do komunikacji z centralą, spełnienie założonych funkcji wykonawczych jest możliwe przez indywidualne zaprogramowanie np. zdalne pulpity obsługowe, szyfratory itd.
7) interfejs sygnalizacyjny (modem) - urządzenie umożliwiające przekazanie sygnałów z centrali do alarmowego centrum odbiorczego (oddalonego) poprzez wykorzystanie różnych systemów transmisji.

System alarmowy, obok uruchomienia sygnalizacji może spowodować dodatkowo uruchomienie takich urządzeń jak:

-gaśnicze - np. tryskacze,

-otwarcia klap dymowych,

-otwarcia wyjść ewakuacyjnych,

- zasłonięcie kurtyn ppoż. dla oddzielenia poszczególnych stref obiektu,

-wyłączenie dopływu prądu elektrycznego do zagrożonego obiektu,

-blokady drzwi dla udaremnienia wycofania się włamywaczy (napastników) z łupem,

-kurtyn (ekranów), krat, żaluzji celem uniemożliwienia kradzieży,

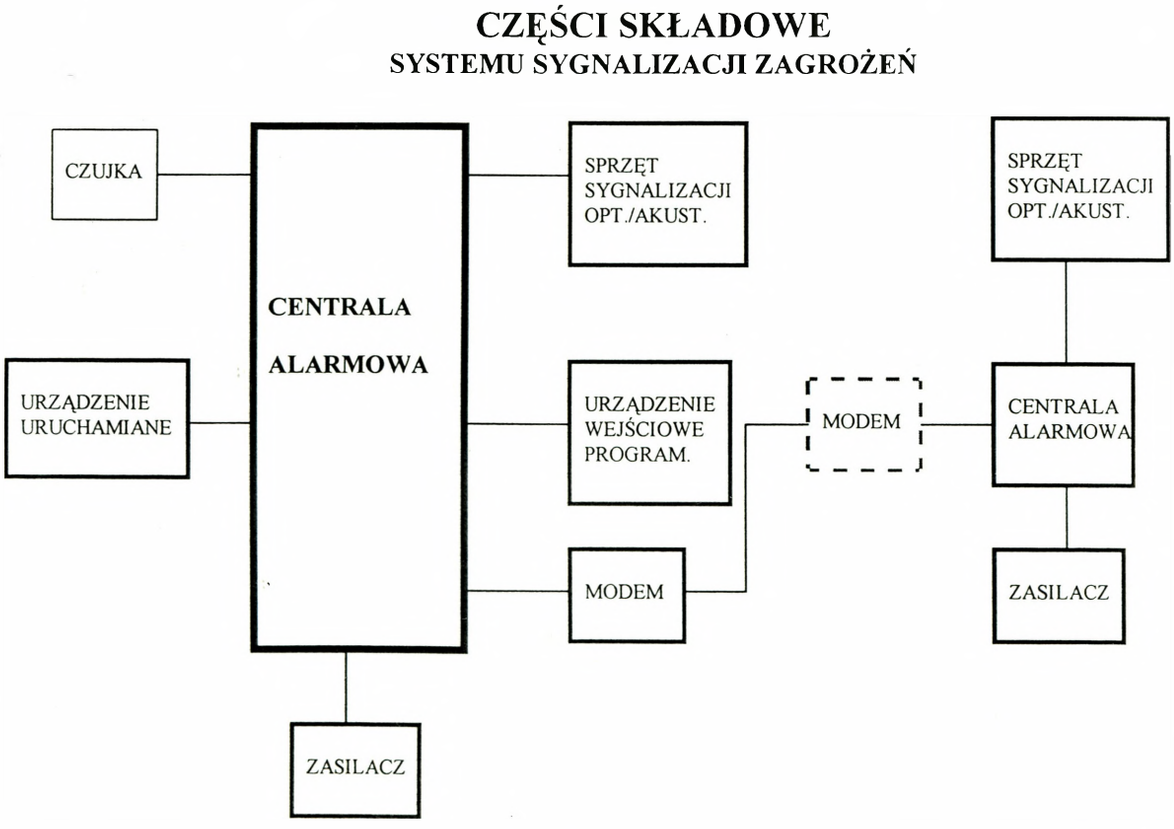
-włączenie oświetlenia,

-nagrywających i dokumentujących proces włamania i kradzieży za pomocą kamer telewizji użytkowej, aparatów fotograficznych, filmowych.

W systemach alarmowych stosuje się następujące typy czujek:

- aktywne podczerwieni- urządzenie wykrywające, przeznaczone do wytwarzania stanu alarmowania, gdy zostanie przerwana wiązka promieniowania między nadajnikiem a odbiornikiem. Widmo promieniowania nadajnika powinno znajdować się poza zakresem widzialnym tj. długość fali większa niż 760 nm.
- ultradźwiękowe czujki Dopplera - urządzenie, które wytwarza stan alarmowania w odpowiedzi na zmianę częstotliwości promieniowania ultradźwiękowego odbitego od poruszającego się obiektu. Promieniowaniem ultradźwiękowym jest tu promieniowanie elektromagnetyczne o częstotliwości większej niż 22 kHz.
- mikrofalowe Dopplera- urządzenie, które wytwarza stan alarmowania w odpowiedzi na zmianę częstotliwości promieniowania mikrofalowego odbitego od poruszającej się osoby.

- pasywnej podczerwieni- czujka wywołująca stan alarmowania w odpowiedzi na zmianę odbieranego natężenia promieniowania podczerwonego, spowodowane, przez obiekty poruszające się w obszarze wykrywania.
- wibracyjne- urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie różnego typu drgań lub wibracji materiału, konstrukcji chronionego obiektu.
- stłuczenia szkła- urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie drgań charakterystycznych pękającego (tłuczonego) szkła.
- mechaniczne i elektromechaniczne urządzenia rozwarciowe, kontaktronowe- urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie przerwania obwodu dozorowego przez wyważenie okien, drzwi itd.
- inne urządzenia- specjalistyczne urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie różnych zjawisk fizykochemicznych np. czujka pojemnościowa, ciśnieniowa itd.
- dualne - urządzenia posiadające wymienione wyżej właściwości dwóch czujek np. ultradźwiękowej i pasywnej podczerwieni.



Rys. 2. Części składowe systemu sygnalizacji zagrożeń

1.3. Wymagania stawiane systemom sygnalizacji zagrożeń

Podstawowe wymagania dotyczące systemów sygnalizacji zagrożeń:

1) System wymaga starannego zaprojektowania.
2) Jeżeli jest to konieczne należy system alarmowy podzielić na strefy lub obwody, w celu jednoznacznego wskazania źródła alarmu.
3) Przy projektowaniu systemu należy starannie rozważyć problem zapewnienia możliwości jego uzupełnienia lub modyfikacji.
4) Liczba czujek przyłączonych do jakiegokolwiek obwodu powinna być określona z uwzględnieniem praktycznej możliwości identyfikacji jego uszkodzenia. Przy czym występujące uszkodzenia nie powinny w sposób znaczący wpływać na części systemu nieuszkodzone.
5) Zaleca się sygnalizować uszkodzenia oddzielnie w centrali.
6) Dla wykrycia uszkodzeń niewykrywalnych przez normalne procedury monitorowania należy określić badania okresowe.
7) System alarmowy powinien być tak zaprojektowany, aby poprawne działanie systemu nie mogło być narażone na uszkodzenia spowodowane manipulowaniem przez osoby nieprzeszkolone.
8) Należy przewidzieć takie środki, żeby sprawdzanie poszczególnych czujek nie powodowało wywołania alarmu i wyłączenia całego systemu alarmowego.
9) System powinien spełniać wymagania w warunkach środowiskowych wewnętrznych jak i na zewnątrz obiektu chronionego, które mogą występować w obiektach chronionych np. wilgoć, gorąco, smary, przemysłowe zanieczyszczenia itd..
10) Lokalizacja urządzeń uruchamianych ręcznie powinna być taka, aby zminimalizować ryzyko ich przypadkowego zadziałania lub zadziałania spowodowanego złośliwie, przy zapewnieniu użytkownikowi łatwego dostępu do nich, przy czym liczbę tych elementów należy zredukować do minimum.
11) Konkretny typ czujki nie może być stosowany do wszystkich zastosowań i ostateczny ich wybór zależy od indywidualnych warunków.
12) W systemie alarmowym należy stosować czujki, które odróżniają, zagrożenie od normalnych warunkach środowiskowych panujących wewnątrz budynku.

13) Czujki powinny być tak rozmieszczone, aby zapewnić bezpieczeństwo wymaganej powierzchni. Montować na pozbawionych wibracji oraz niedostępnych dla osób niepowołanych.

14) Wszelkie justowania i nastawienia powinny wymagać użycia specjalistycznego narzędzia. Należy rozważyć możliwość zasłonięcia czujki przez zmiany w architekturze pomieszczenia chronionego.

15) Czułość czujki powinna być tak dobrana, aby zapewnić niezbędny stopień ochrony bez wywoływania fałszywych alarmów spowodowanych warunkami środowiskowymi.

16) Centrala alarmowa powinna mieć urządzenie do odbioru, kontroli, zapisu i przekazywania sygnałów z urządzeń wyzwalających, przyłączonych do niej oraz do uruchomienia alarmowych sygnalizatorów akustycznych i alarmowych urządzeń sygnalizacyjnych. System powinien jednoznacznie wskazywać źródła alarmu i sygnalizować oddzielnie stan alarmu i uszkodzeń.

17) System alarmowy powinien posiadać warunki do transmisji sygnałów alarmowych do oddalonego centrum nadzorczego, a także przewidziane urządzenie do transmisji ostrzeżenia o uszkodzeniach.

18) Tor sygnalizacyjny wychodzący poza obiekty dozorowane powinien być umieszczony w ziemi lub ukryty. Łącze telekomunikacyjne trwale połączone z oddalonym centrum powinno być ciągle monitorowane ze wskazaniem w stacji odbiorczej uszkodzenia w razie awarii.

19) W przypadku przeciwstawnych wymagań przy stosowaniu systemów alarmowych mieszanych należy przyznać priorytet wymaganiom ochrony życia np. napad.

2. WYMAGANIA TECHNICZNO - PRAWNE

2.1. Podstawowe uwarunkowania prawne

Wszystkie urządzenia i systemy, które mają być zainstalowane w obiektach chronionych muszą spełniać określone wymagania techniczne i prawne. Zgodnie z art. 7 ustawy z dnia 23.listopada 1990 r. o łączności (Dz.U. nr 86, poz. 504 z póź. zm.) zakładane i używane na terytorium Rzeczpospolitej Polskiej urządzenia i systemy telekomunikacyjne (w tym również urządzenia przesyłające systemy alarmowe) powinny mieć wydane przez ministra łączności świadectwo dopuszczenia do eksploatacji, zwane świadectwem homologacji. Ponadto na podstawie zarządzenia ministra spraw wewnętrznych z 28 marca 1994 r. w sprawie wprowadzenia obowiązku stosowania Polskich Norm i norm branżowych (Dz.U. nr 44, poz. 174) polska norma PN-93/E-08390 Systemy alarmowe - stała się obowiązkowa.

Polskie Normy, zgodnie z treścią ustawy z 3 kwietnia 1993 r. o normalizacji (Dz.U. nr 55, poz. 251) określają wymagania, metody badań oraz metody i sposoby wykonywania innych czynności, w szczególności w zakresie bezpieczeństwa pracy i użytkowania oraz ochrony życia życia, zdrowia i mienia. Spełnienie wymagań określonych w stosownych przepisach potwierdzano do niedawna zaświadczeniem kwalifikacyjnym, zwanym Atestem wydawanym przez Zakład Rozwoju Technicznej Ochrony Mienia TECHOM w Warszawie, upoważniony do tych badań na podstawie zarządzenia nr 20 prezesa Polskiego Komitetu Normalizacji Miar i Jakości z 15 kwietnia 1986 r. w sprawie ustalenia wykazu mechanicznych i elektronicznych urządzeń zabezpieczających podlegających badaniom, ocenie i kwalifikacji oraz wykazu jednostek organizacyjnych powołanych i upoważnionych do tych działań (Dziennik Normalizacji i Miar nr 4, poz. 8 z póź. zm.). Zarządzenie to zostało wydane na postawie ust. 5 postanowienia nr 17 Prezydium Rządu z 18 lutego 1985 r. w sprawie technicznej ochrony mienia.

1 stycznia 1994 r. na mocy ustawy z 3 kwietnia 1993 r. o badaniach i certyfikacji (Dz.U. nr 55, poz. 250) rozpoczął funkcjonowanie krajowy system badań i certyfikacji wyrobów i usług oraz działające w nim Polskie Centrum Badań i Certyfikacji, akredytowane

laboratoria badawcze i jednostki certyfikujące. Tym samym postanowienie nr 17/85 Prezydium Rządu z mocy prawa przestało obowiązywać. Obecnie zastosowanie mają postanowienia cytowanej ustawy o normalizacji, ustawy o badaniach i certyfikacji oraz akty wykonawcze wydane na ich podstawie. Przepisy te nie nakładają obowiązku dokonywania badań, oceny i kwalifikacji urządzeń stosowanych w „ochronie mienia i osób"; nie podlegają one obowiązkowej certyfikacji. Natomiast zgodnie z art. 217 kodeksu pracy - producent, importer czy instalator urządzeń i systemów zabezpieczeniowych ma obowiązek wydać deklaracje zgodności tych wyrobów z normami. W odniesieniu do systemów alarmowych praktycznie jedyną formą potwierdzania omawianej zgodności jest wydanie deklaracji zgodności w sposób określony w normie PN EN-45014:1989.

2.2. Współdziałanie Stacji Monitorowania Alarmów (SMA) z organami bezpieczeństwa i porządku publicznego.

W omawianych rozwiązaniach techniczno-organizacyjnych istotną rolę będą odgrywały zasady współdziałania policji ze stacjami SMA obejmujące zespół przedsięwzięć organizacyjno-wykonawczych, zmierzających do skoordynowania działań prowadzonych przez policję i komercyjne firmy ochrony dla jak najlepszego osiągnięcia celu, którym jest możliwość zapewnienia natychmiastowej reakcji sił interwencyjnych na sygnał alarmowy. Można to osiągnąć przez umiejętne łączenie i skuteczne wykorzystywanie możliwości obu stron dla optymalizacji tych działań. Zagadnienia dotyczące współdziałania w tym zakresie określa m.in. Polska Norma systemy alarmowe, która precyzuje m.in.:

1) w p. 5.2.1 ark. 11: „...wymagania dotyczące alarmowania powinny być ustalone tak dokładnie, jak to jest możliwe, przez konsultacje między zainteresowanymi stronami, tj. zamawiającym, konsultantem, dostawcą sprzętu alarmowego, instytucją nadzorującą alarmowe centrale odbiorcze, służbami telekomunikacyjnymi, lokalną policją lub służbami pożarowymi...";
2) w p. 5.2.2 ark. 11: „...w celu zapewnienia transmisji sygnałów do alarmowego centrum odbiorczego, przed ich dołączeniem należy dokonać uzgodnień między zainteresowanymi stronami w celu określenia informacji, jaka ma być przekazywana, oraz działań, które mają być podjęte po odbiorze sygnałów: alarmowego, uszkodzeniowego, testującego lub innych";

3) w p. 7 ark. 14: „Należy ustalić procedury postępowania z alarmami, ostrzeżeniami o uszkodzeniu, wyłączeniu części lub całego systemu alarmowego ze stanu działania. Procedury te powinny być zatwierdzone przez odpowiednie władze przed ich wprowadzeniem". Pod pojęciem odpowiednie władze należy rozumieć wyznaczone władze odpowiedzialne za zajmowanie się dozorowanymi obiektami po wystąpieniu stanu alarmowania i za podejmowanie odpowiedniego działania;
4) w p. 6 ark. 14: „8. Działanie w przypadku alarmu. Działanie to powinno być określone z góry i ustalone w ścisłym porozumieniu z organizacjami, które posiadają doświadczenie lub władzę w tych dziedzinach oraz są kompetentne do określenia wszystkich czynników, które należy wziąć pod uwagę przy podejmowaniu decyzji o tym, jakie działania należy przedsięwziąć w przypadku alarmu i jakie urządzenia sygnalizacyjne są wymagane do jego podtrzymania. Odpowiedni personel powinien być poinstruowany o właściwym inicjowaniu stanu alarmowania i wszelkich działaniach, które należy podjąć w przypadku zaistnienia alarmu".

Niezależnie od wymienionych unormowań prawnych, w wypadku lokalizacji komercyjnych SMA poza jednostkami policji, w celu przyspieszenia przekazania informacji do policji o stwierdzonym zagrożeniu lub popełnieniu przestępstwa, można - w miarę istniejących możliwości technicznych - rozważać:

- wykonanie tzw. łącza sztywnego między policją a SMA,
- zainstalowanie w jednostce policji urządzenia radiowego SMA, na koszt SMA i zgodnie z zasadami obowiązującymi w resortowej sieci łączności albo - wydzielenie specjalnego numeru telefonu wewnętrznego w jednostce policji na potrzeby monitoringu.

Ponadto, gdy na danym terenie usługi monitoringu świadczy kilka firm, jednym z możliwych rozwiązań jest zainstalowanie w policji urządzenia odbierającego informacje już „obrobione" przez SMA w jednolitej ustalonej formie.

Szczegółowe zasady współdziałania między policją a załogami ochronnymi sprawującymi nadzór nad obiektami chronionymi, patrolami lub grupami interwencyjnymi firm komercyjnych na informację podaną przez SMA o zaistnieniu zdarzenia przestępczego, można opracować indywidualnie, uwzględniając specyfikę i potrzeby. Opracowanie to powinno wynikać z dostosowania i modyfikacji odpowiednich procedur przesłanych do wszystkich komendantów policji.

Jedną z podstawowych czynności jest dokumentowanie zdarzeń związanych z monitoringiem. Wszyscy uczestnicy tego przedsięwzięcia powinni dla własnego dobra prowadzić rzetelną dokumentację. Szczegóły można znaleźć w cytowanej polskiej normie.

Wszyscy zainteresowani funkcjonariusze policji zostali zapoznani z odpowiednimi technikami i taktyką interwencji w tych zdarzeniach. Ponadto w skład grupy dochodzeniowo - śledczej udającej się na miejsce zdarzenia gdy „złamano system" i dokonano czynu przestępczego - wchodzą odpowiednio przygotowani eksperci policyjni, posiadający uprawnienia rzeczoznawców systemów alarmowych lub biegłych sądowych.

2.3. Zakres odpowiedzialności karnej

Na zakończenie sprawa najmniej przyjemna, tj. zasady odpowiedzialności karnej, cywilnej itp.

1) **Odpowiedzialność karna wynikająca z ustawy o łączności.** Zgodnie z art. 86 ustawy z 23 listopada 1990 r. o łączności (Dz.U. nr 86, poz. 504) ustawa z 20 maja 1971 r. - kodeks wykroczeń (Dz.U. nr 12, poz. 114) w art. 63 brzmi:

„ § 2. Tej samej karze podlega, kto bez wymaganego zezwolenia lub homologacji zakłada bądź używa urządzenia, linie lub sieci telekomunikacyjne, radiowe urządzenia nadawcze i nadawczo-odbiorcze albo bez wymaganego przydziału wykorzystuje częstotliwość.

§ 3. Można orzec przepadek przedmiotów służących do popełnienia czynów określonych w § 1 i 2, choćby nie stanowiły własności sprawcy".

2) **Odpowiedzialność karna wynikająca z ustawy o normalizacji.** W rozdziale 6 ustawy z 3 kwietnia 1993 r. o normalizacji (Dz.U. nr 55, poz. 251) zawarto przepisy karne:

„Art. 23. Osoba odpowiedzialna za działalność produkcyjną lub usługową albo za kontrolę jakości, która nie przestrzega wymagań Polskich Norm, w stosunku do których wprowadzono obowiązek ich stosowania w trybie art. 19 ust. 2 lub 3 bądź też nie zachowuje warunków określonych w decyzji zezwalającej na odstąpienie od obowiązku stosowania norm:

1) w produkcji wyrobów przeznaczonych do obrotu oraz przy wprowadzaniu ich do obrotu,

2) w obrocie wyrobami do czasu dokonania odbioru przez pierwszego użytkownika lub konsumenta albo do terminu określonego w normie,

3) przy wykonywaniu czynności objętych normami,

– podlega karze grzywny.

Art. 24. Osoba odpowiedzialna za działalność produkcyjną lub usługową albo za kontrolę jakości, która dopuszcza do wydania deklaracji zgodności z normą niezgodnie ze sposobem i warunkami ustalonymi na podstawie art. 20 podlega karze grzywny.

Art. 22. Orzekanie w sprawach o czyny wymienione w art. 23 i 24 następuje w trybie przepisów kodeksu postępowania w sprawach o wykroczenia."

3) Odpowiedzialność ekonomiczna za naruszenie reguł certyfikacyjnych. Ustawa z 3 kwietnia 1993 r. o badaniach i certyfikacji (Dz.U. nr 55, poz. 250) w rozdziale 6 określa dwa czyny zabronione, których dokonanie grozi zastosowaniem sankcji ekonomicznych w postaci obowiązku wpłaty do budżetu państwa należnych kwot pieniędzy.

Art. 26 ust. 1 ustawy określa odpowiedzialność z tytułu niewłaściwego postępowania z wyrobem podlegającym obowiązkowej certyfikacji (art. 13 ust. 1 ustawy). „Jeżeli podmiot gospodarczy wprowadzi do obrotu wyroby podlegające oznaczeniu znakiem bezpieczeństwa lecz nie oznaczone tym znakiem lub wprowadzi do obrotu wyroby wyprodukowane niezgodnie z wymaganiami stanowiącymi podstawę do przyznania prawa stosowania znaku bezpieczeństwa, to jako sankcję ekonomiczną ma obowiązek wpłacić do budżetu państwa kwotę stanowiącą 100% sumy uzyskanej ze sprzedaży zakwestionowanych wyrobów". Natomiast art. 26 tejże ustawy tak samo stanowi w stosunku do podmiotu gospodarczego, który wykona usługę nie posiadając wymaganego certyfikatu na system jakości lub wykona usługę niezgodnie z wymaganiami stanowiącymi podstawę wydania certyfikatu na system jakości. Ustawa o badaniach i certyfikacji określa postępowanie szczególne związane z odpowiedzialnością podmiotów gospodarczych, które dokonały działań zabronionych.

4) Odpowiedzialność cywilna Stacji Monitorowania Alarmów wynikająca z umów prawa zobowiązaniowego. Umowy zawierane między komercyjnymi firmami ochrony prowadzącymi działalność gospodarczą w zakresie usług związanych z monitorowaniem sygnałów alarmowych a ich abonentami - są umowami prawa zobowiązaniowego i kwestie te regulują przepisy kodeksu cywilnego i dotyczą tych dwóch stron.

5) Odpowiedzialność cywilna właściciela systemu w rozumieniu art. 471 i 472 kodeksu cywilnego. W ramach realizacji swoich zadań policja jest uprawniona do domagania się, aby właściciele systemów alarmowych utrzymywali te urządzenia na należytym poziomie technicznym m.in. w celu eliminowania przypadków fałszywych alarmów. Natomiast na gruncie obowiązujących przepisów prawa cywilnego istnieje pełna podstawa do domagania

się od właścicieli systemów sygnalizacji alarmowych podłączonych do jednostek policji zwrotu kosztów interwencji policyjnej podjętej w wyniku fałszywego alarmu. Dlatego też za każdorazowe nieuzasadnione wezwanie policji do obiektu, którego urządzenia odbierające sygnały alarmowe zainstalowane są w jednostkach policji bądź zgłoszenie otrzymane ze SMA, ustala się karę umowną w zryczałtowanej kwocie pieniężnej będącej sumą odpowiednich stawek finansowych. Należności z tytułu kar uiszczane będą kwartalnie, a uzyskane wpływy przekazywane będą na budżet państwa.

3. WSPÓŁCZESNE SYSTEMY SYGNALIZACJI ZAGROŻEŃ

W tym rozdziale zostaną przedstawione przykładowe rozwiązania charakteryzujące współczesne systemy sygnalizacji zagrożeń. Na przykładzie systemu ochrony i monitoringu obiektów oraz systemu wizyjnego pokazane zostaną cechy i tendencje rozwojowe tych systemów. W pkt. 3.3. przedstawiono dwie różne metody realizacji systemów powiadamiania i alarmowania (na bazie istniejącej sieci telefonicznej i z wykorzystaniem systemów pagingowych. Nie sposób w tym rozdziale przedstawić wszystkich rozwiązań obecnie stosowanych. Jest to temat bardzo rozległy i wymagałby wielotomowej monografii.

3.1. System ochrony i monitoringu wykorzystujący sieć radiową

W ostatnim okresie coraz większą popularność zdobywają systemy ochrony i monitoringu obiektów wykorzystujące łącza radiowe do transmisji sygnałów alarmowych do Centrum Nadzoru. Zadaniem systemu jest bezprzewodowy nadzór nad wieloma obiektami chronionymi wyposażonymi w lokalne systemy alarmowe.

W skład systemu wchodzą:[2]

a) nadajniki radiowe umieszczone w obiektach chronionych. Mogą być one połączone do dowolnych lokalnych systemów alarmowych (zasilanie 12V).

b) Stacja monitorowania składająca się z odbiornika radiowego oraz odpowiedniego oprogramowania komputerowego typu IBM PC.

Na ekranie monitora uzyskać można następujące informacje o stanie systemu:

- wzbudzone alarmy (napad, włamanie, pożar, zagrożenie życia),
- stan łączności z poszczególnymi abonentami,
- dane abonentów,
- opis obiektów chronionych, dróg dojazdu,

Ponadto stacja monitorowania prowadzi automatyczną ewidencję zagrożeń dotyczących konkretnego obiektu (historia abonenta) oraz alarmów wykrytych przez system (raport).

---

[2] W tym przykładzie wykorzystano rozwiązania techniczne firmy Nokton specjalizującej się w radiowych systemach zbiorowej ochrony mienia.

Najważniejsze parametry:

- zasięg działania: w promieniu do 25 km od stacji monitorującej,
- pojemność systemu: ok. 250 abonentów na jeden kanał radiowy,

Wymagania na sprzęt komputerowy:

- minimalna konfiguracja PC 386SX 40MHz, FDD 1.44Mb, VGA, HDD 40MB,
- MS-DOS 5.0 lub wyższy,
- zalecane zasilacz bezprzerwowy UPS do komputera (konieczny w przypadku częstych zaników napięcia sieci oraz drukarka.

W porównaniu do systemów kablowych systemy radiowe są łatwe w obsłudze i szybkie w montażu oraz tańsze. Zawierają one takie same elementy (centrale alarmowe, czujki, itp.) jak „klasyczne" kablowe systemy monitoringu.

Zaletą większości tego typu rozwiązań jest możliwość późniejszego podłączenia centralek alarmowych przewodami w celu zapewnienia większej niezawodności systemu.

Zasadniczą wadą takich systemów jest ograniczone pasmo sygnałów radiowych, a w związku z tym monitoringowi radiowemu może podlegać tylko ściśle określona liczba obiektów do ochrony.

3.2. System ochrony i monitoringu wykorzystujący sieć energetyczną

Bardzo oryginalnym rozwiązaniem jest system ochrony i monitoringu obiektów wykorzystujący linie energetyczne. System te wykorzystuje standardowe centrale alarmowe, czujki i inne elementy ochrony obiektów. Oto krótka charakterystyka tego systemu.[3]

Każda z centralek komunikuję się z komputerem w punkcie dozoru za pośrednictwem sieci 220V. W przypadku, gdy łączność z pewną grupą pomieszczeń nie jest możliwa taką drogą ze względu na duży poziom zakłóceń lub wyjątkowo duże tłumienie sygnału w sieci, istnieje możliwość ułożenia oddzielnej linii przewodowej. Jedna para przewodów wykorzystywana jest wówczas dla wielu centralek.

Odporność na próby sabotażu

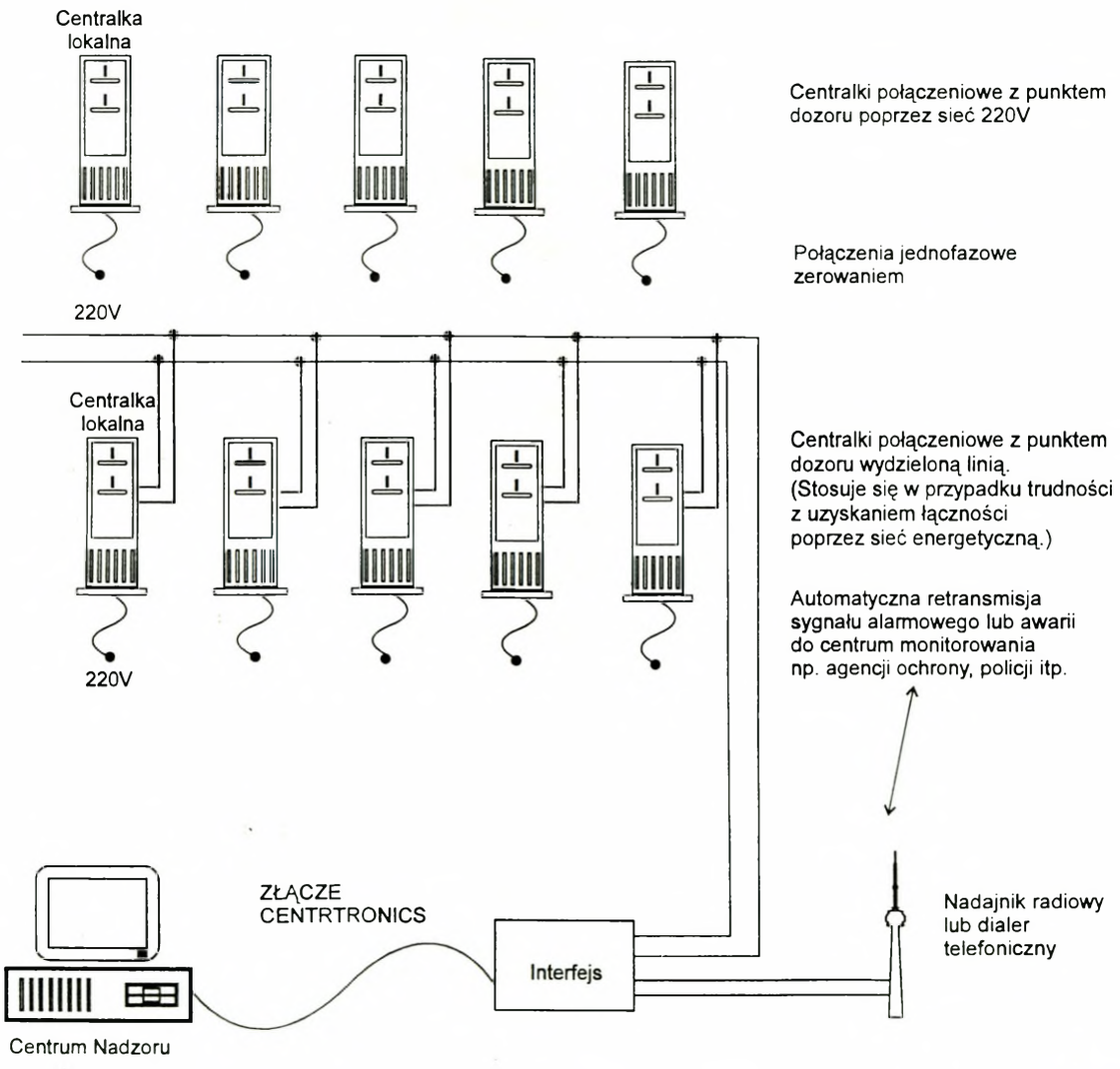
System jest wyposażony w klasyczną ochronę przed sabotażem w postaci pętli antysabotażowej. Dodatkowo omówienia wymaga zagadnienie odporności na próby

[3] Jest to system opracowany całkowicie przez polskich konstruktorów.

przerwania łączności pomiędzy centralkami a punktem dozór. Przestępcy najczęściej próbują uniemożliwić łączność np. poprzez:

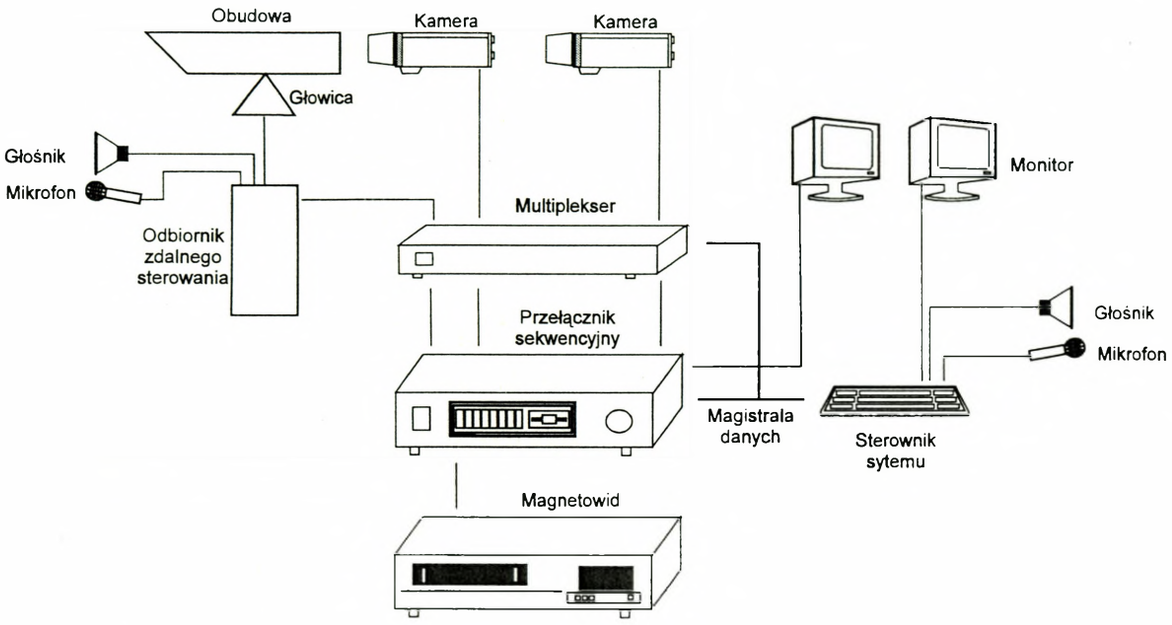
- odłączenie zasilania (wykręcenie bezpieczników);
- przerwanie ciągłości przewodów sieci 220V;
- zwieranie przewodów sieciowych;
- wprowadzenie do sieci sygnałów zakłócających;

W przypadku odłączenia zasilania budynku jeżeli nie została przerwana ciągłość przewodów między punktem dozoru i centralkami, system działa nadal dzięki zasilaniu awaryjnemu, natomiast warunki łączności są nadal lepsze niż przy normalnej pracy, gdyż wyeliminowane zostaną zakłócenia od innych urządzeń elektrycznych.



Rys. 3. Przykład współczesnego systemu ochrony i monitoringu obiektów wykorzystującego sieć energetyczną do transmisji sygnałów alarmowych.

3.3. System wizyjny



Rys. 4. Przykład nowoczesnego systemu telewizji użytkowej

Nowoczesne systemy telewizji użytkowej mogą być wyposażone w zależności od systemu nawet do 1024 kamer. Kamery są sterowane przy pomocy sterownika systemu (pulpit operatora). Moduł multipleksera przekazuje sygnały z kamer do magnetowidu zapisu poklatkowego który rejestruje sygnały na taśmie magnetycznej. Przełącznik sekwencyjny przełącza sygnały pochodzące od kamer według programu wprowadzonego przez operatora, obrazy z tych kamer przekazywane są do monitorów.

Podstawowe funkcje systemu[4]

- ciągła rejestracja obrazu z kamer na magnetowidach;
- ciągła analiza poklatkowa, cyfrowa rejestracja obrazu;
- odtwarzanie obrazów zarejestrowanych na magnetowidach;
- sterowanie ruchem kamer umieszczonych na głowicach obrotowych;
- zmiana powiększenia obrazu dla kamer posiadających obiektyw typu zoom;
- programowe ustawienie detektorów pobudzających cyfrową rejestrację obrazu;

[4] Przykładowe rozwiązanie firmy effeff - Fritz Fuss GmbH.

- podział na dwa typy pracy: pełny i z ograniczony nadzór;
- ustawienie obszarów aktywności detektorów ruchu;
- szybkie odtwarzanie zarejestrowanych poklatkowych obrazów bez przerywania analizy i cyfrowej rejestracji obrazów;
- wyszukiwanie zarejestrowanych obrazów po nazwie kamery i czasie rejestracji obrazów;
- dynamiczne ustawianie sposobu wyświetlania obrazów aktualnych z kamer na monitorach;
- dynamiczna zmiana parametrów działania i konfiguracji systemu;
- wyświetlanie planów obiektu;
- przedstawienie rozmieszczenia kamer na planach;
- drukowanie obrazów na planach;
- drukowanie obrazów zarejestrowanych na taśmie magnetowidowej;
- drukowanie cyfrowo zarejestrowanych obrazów;

Opcjonalne funkcje systemu

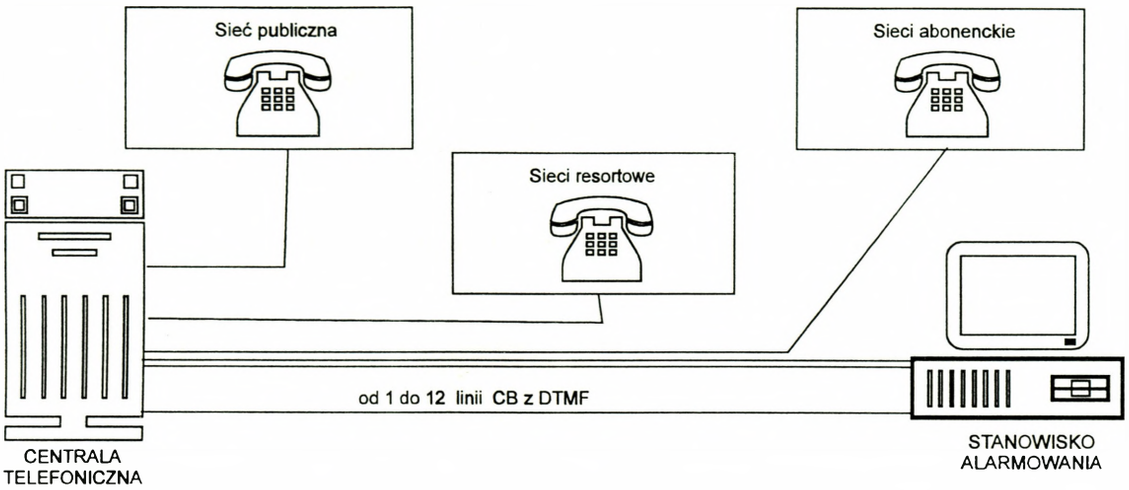
- identyfikacja wejściowych kart;
- baza danych o incydentach chuligańskich i osobach biorących w nich udział;
- dostęp do danych zgromadzonych w bazie w różnych miejscach obiektu;
- rejestracja i wyświetlanie stanów zabezpieczeń (alarmowych, kontroli dostępu, pożarowych);
- sterowanie urządzeniami zewnętrznymi (stany alarmowe siłowniki bram wjazdowych);
- otwieranie i zamykanie przejść ewakuacyjnych;
- powiadamianie Policji i Straży Pożarnej w sytuacjach alarmowych;
- rozbudowa na nowe moduły, bez konieczności wymiany istniejących rozwiązań;

3.4. Systemy powiadamiania i alarmowania

System wykorzystujący sieć telefoniczną

Nowoczesne systemy powiadamiania i alarmowania oferują powiadamianie określonej grupy abonentów za pośrednictwem sieci telefonicznej. Baza danych abonentów powiadamianych znajduje się w komputerze podłączonym do centrali telefonicznej. Komunikat może być wysłany do dowolnego abonenta dysponującego aparatem telefonicznym.

Możliwości nowoczesnego systemu powiadamiania i alarmowania zostaną przedstawione na przykładzie systemu DGT-TSA2.



Rys. 5. Schemat połączeń systemu DGT-TSA2

Telefoniczny system alarmowania DGT-TSA-2 umożliwia powiadamianie określonych grup abonentów za pośrednictwem sieci telefonicznej. Komunikat może być wysyłany do dowolnego abonenta dysponującego aparatem z sygnalizacją DTMF tonowa). System jest w pełni zautomatyzowany i posiada zabezpieczenia kodowe przed dostępem osób nieupoważnionych. Oprogramowanie do obsługi systemu działa w środowisku WINDOWS 95.

System DGT-TSA-2 zapewnia:

- możliwość powiadamiania abonenta dowolnej centrali telefonicznej
- pełna rejestracja wszystkich czynności od momentu uruchomienia systemu
- obserwacja wyników alarmowania abonentów w czasie rzeczywistym
- odsłuchanie alarmu tylko po podaniu hasła,
- rozbudowana strategia powiadamiania (czy powtarzać alarm, ile razy, liczba odtworzeń komunikatu),
- tworzenie grup powiadamiania abonentów,
- różne tryby zakończenia alarmu (automatyczne, na żądanie operatora, po zaprogramowanym czasie),
- wydruk listy abonentów,
- automatyczny start alarmu po uruchomieniu aplikacji z parametrem wywołania

- inicjowanie alarmu z innego komputera.

System DGT-TSA2 współpracuje z dowolną centralką telefoniczną. W skład operatorskiego stanowiska powiadamiania wchodzi:

- komputer PC z mikrofonem,
- karta telefoniczna DIALOGIC połączoną z centralą łączami CB z DTMF (opcjonalnie od 1 do 12 łączy, standardowo 4)
- specjalistyczne oprogramowanie systemu DGT-TSA pracuje w środowisku WINDOWS 95

Baza danych powiadamiania systemu DGT-TSA-2 zawiera zestaw danych poszczególnych abonentów;

- nazwisko i imię
- tytuł stopień stanowisko
- adres
- strategia powiadamiania(oddzielna dla każdego numeru)
- hasła (do identyfikacji abonenta)
- może zawierać inne dane w zależności od potrzeb.

Zestaw komunikatów słownych

W systemie można wcześniej przygotować zbiór różnych komunikatów, z których operator przed rozpoczęciem sesji wybiera odpowiedni.

Sesja powiadamiania

Sesje alarmowania uruchamia upoważniona osoba (np. oficer dyżurny) po wybraniu właściwej grupy i komunikatu, który ma zostać nadany.

W trakcie sesji alarmowej na stanowisku powiadamiania na bieżąco prezentowany jest stan łączy wszystkich powiadamianych abonentów.

Zakończenie sesji alarmowej następuje:

- automatyczne - po przyjęciu wiadomości przez wszystkich abonentów,
- po zaprogramowanym czasie,
- ręcznie w wyniku decyzji operatora.

Historia każdej sesji jest zapamiętywana w zbiorze dyskowym. W danym momencie możliwe jest przeanalizowanie wybranej sesji, a także filtrowanie danych (abonenci nie

powiadomieni, łącza uszkodzone itp.) tworzenie i drukowanie zestawień (liczebność grupy, liczba wywołań przyjętych , łączy uszkodzonych, średni i maksymalny czas zgłaszania itp.)

Systemy pagingowe

Jednokierunkowy, radiowy system komunikacyjny, umożliwiający abonentowi wyposażonemu w niewielki i tani odbiornik kieszonkowy (pager) otrzymywanie krótkich komunikatów przywoławczych.

Ze względu na zasięg rozróżnia się:

- systemy lokalne, dla prywatnych sieci, stosowane zwykle w obrębie jednego przedsiębiorstwa i mające jeden lub kilka zsynchronizowanych nadajników małej mocy;
- systemy o dużym zasięgu, obejmujące obszar miasta, regionu lub kraju, nadzorowane przez operatorów publicznych.

Ze względu na rodzaj przesyłanej informacji i związanej z tym konstrukcji terminali odbiorczych rozróżnia się systemy przywoławcze informujące abonenta:

- sygnałem tonowym, bez dodatkowych informacji: o nadawcy, o rodzaju sprawy, pilności rozmowy;
- sygnałem numerycznym na wyświetlacz użytkownika, przesyłanym łącznie z sygnałem tonowym;
- sygnałem alfanumerycznym ukazującym się na ekranie ciekłokrystalicznego wyświetlacza tekstowego.

W Polsce działa już dziesięć lokalnych firm pagingowych. i jedna ogólnopolska: Polpager. Z systemów przywoławczych korzystają najczęściej firmy budowlane, transportowe, usługowe, banki, służby miejskie, rzadziej prywatni abonenci.

Systemy pagingowe są w Polsce mało popularne, ze względu na słabą infrastrukturę telekomunikacyjną kraju (zbyt mała ilość publicznych aparatów telefonicznych), żeby skontaktować się z daną osobą po otrzymaniu krótkiego komunikatu na wyświetlaczu. Tego typu systemy zaczynają być popularne w firmach, instytucjach itp. A przecież jest to znacznie tańsza alternatywa dla telefonii komórkowej i w krajach Europy Zachodniej prawie każde dziecko posiada taki tani pager aby go np. przywołać do domu na obiad. W przypadku, gdy firma zarządza swoim systemem (jest jego operatorem), koszty wybudowania takiego systemu

są jednorazowe i niewielkie: wybudowanie nadajnika, połączenia go z centralą miejską (zakładową) i wyposażenie pracowników w pagery.

W ostatnich latach w Polsce coraz większą popularność zdobywają systemy pagingu prywatnego.[5] Są przydatne zwłaszcza w przedsiębiorstwach i instytucjach, których pracownicy, przebywając na zamkniętym obszarze, stale się przemieszczają.

System pagingu prywatnego może np. zawiadywać urządzeniami gaśniczymi i alarmowania. Bez udziału człowieka (po połączeniu z czujnikami) potrafią włączać syreny, oświetlenie alarmowe, urządzenia gaśnicze, a także powiadamiać straż pożarną czy inne służby.[6]

W dobie szybkiego rozwoju publicznych sieci przywoławczych powstaje pytanie- czemu inwestować znaczne środki w budowę własnych systemów. Można powiedzieć, że są cztery główne powody, by jednak uruchomić sieć prywatną .

Koszty

Nie są wysokie. W sieciach o ograniczonym zasięgu, na przykład działających w hotelach. szpitalach czy na terenie zakładów o niewielkiej liczbie pagerów (kilkadziesiąt), inwestycja w infrastrukturę zwraca się w ciągu pół roku - nie ponosi się przecież kosztów utrzymania.

Pokrycie

Na niektórych obszarach pokrycie sieci publicznych jest słabe. Instalacja prywatnego systemu jest wtedy jedynym sposobem na zapewnienie sobie pewnej łączności jednodrożnej.

Kontrola

---

[5] Mianem pagingu prywatnego są określane systemy pagingowe stosowane na użytek wewnętrzny instytucji, firmy itp. Instytucja, która posiada taki system jest jego operatorem.

[6] W latach 90-tych obrona cywilna i służby ratownicze Republiki Czeskiej stanęły wobec problemu przestarzałego mało efektywnego i kosztownego w utrzymaniu ogólnokrajowego systemu ostrzegawczego. Kilka tysięcy syren alarmowych kontrolowano poprzez zawodne linie telefoniczne.

Koszty utrzymania - w związku z ciągłymi awariami rosły w każdym miesiącu. Odnośne władze zaczęły zatem poszukiwać kompleksowego rozwiązania i zwracać się do producentów tego rodzaju systemów. Swoją ofertę w 1994 roku przedstawiła również Motorola - był nią system ostrzegawczo- alarmowy CAS 100 - był to system pagingowy.

Kwatera główna czeskiej obrony cywilnej zdecydowała się na zakup systemu, mając na uwadze krótki czas zwrotu inwestycji.

Pierwotnym przeznaczeniem sieci była kontrola syren ostrzegawczych, ale system zaczął służyć także przekazywaniu informacji członkom służb ratowniczych. Dzięki nim informacja jest przekazywana szybko i dokładnie. Czeski CAS 100 korzysta z pagerów alfanumerycznych.

System CAS 100 ma jeszcze jedną ważną zaletę: transmisja odbywa się w formie cyfrowej, nie może być wykryta i podsłuchana czy zakłócana bez użycia najbardziej zaawansowanych urządzeń wojskowych. Sieć jest więc jest odporna na zwykłe środki walki elektronicznej.

CAS 100 to system oparty na technologii komputerowej - wszystkie wiadomości instrukcje procedury mogą być zachowane w pamięci komputera, więc dostęp do nich jest błyskawiczny. Obrona cywilna Republiki Czeskiej sukcesywnie wprowadza CAS 100 na terenie całego kraju. System został przedstawiony ekspertom i szerokiej publiczności na zeszłorocznej wystawie sprzętu ochronnego i ratowniczego PRAGOSEC w Pradze.

Każdy system wymaga konserwacji i serwisu. Jeżeli system przywoławczy służy powiadamianiu alarmowemu w najważniejszej sytuacjach (ratowanie życia i mienia), jego użytkownik (operator) musi mieć nad tym pełną kontrolę.

Szybkość

W sytuacjach pagingu prywatnego komunikat jest przesyłany natychmiast. Prędkość reakcji systemu nie zależy od liczby wiadomości w danej chwili i sprawności operatora.

Cechy współczesnych systemów sygnalizacji zagrożeń

Z przedstawionych charakterystyk współczesnych systemów wynika, że cechują się one: dużą ilością przesyłanej informacji, łatwością obsługi, niezawodnością, skrytością i bezpieczeństwem przesyłanej informacji, itp.

Dąży się do tego aby system ochrony obiektów był nadzorowany przez jak najmniejszą liczbę osób. Operator systemu jest w stanie nadzorować ochronę obiektów położonych w znacznej odległości od siebie. Za pomocą odpowiedniego oprogramowania system ochrony jest w stanie sprawdzać stan zabezpieczenia w każdym obiekcie. W przypadku jakiegokolwiek alarmu automatycznie przedstawia obraz obserwowanego obiektu na monitorze oraz sygnalizuje sygnałem dźwiękowym. Obrazy z wszystkich kamer są rejestrowane na taśmie magnetycznej przy pomocy magnetowidu zapisu poklatkowego.

Obecne tendencje rozwojowe systemów ochrony obiektów dążą do integracji różnych systemów:

- systemu telewizji użytkowej;
- systemu sygnalizacji włamań i napadów;
- systemu sygnalizacji pożaru
- systemu kontroli dostępu i innych.

Przy opracowaniu programów komputerowych położono duży nacisk na prostotę ich obsługi. Osoby których zadaniem będzie wyłącznie obsługa zdarzeń (a więc strażnicy lub portierzy) mogą nauczyć się tego w bardzo krótkim czasie wystarczy im znajomość położenia na klawiaturze klawiszy Entera i Esc. Natomiast wprowadzenie do programu danych chronionych pomieszczeń, dokonywanie zmian konfiguracji itp. wymaga oczywiście przynajmniej w pewnym stopniu obeznania z obsługą komputerów i zaznajomienia z programem. Wykonują to osoby odpowiedzialne za konserwację systemów alarmowych.

W punkcie nadzoru z komputera można sterować następującymi funkcjami centralek:

- uzbrajaniem i rozbrajaniem centralek alarmowych,
- włączaniem i wyłączaniem zewnętrznego przekaźnika, który może być wykorzystany np. do sterowania oświetleniem czy ogrzewaniem,
- włączanie i wyłączanie syreny alarmowej,
- włączaniem i wyłączaniem buzzera (sygnalizatora akustycznego) np. w celu przywołania osoby, gdy w budynku brak jest wewnętrznej sieć telefonicznej,
- sterowanie wymienionymi funkcjami odbywa się z potwierdzeniem tzn. centralka przesyła zwrotne informacje o swoim stanie,
- sprawdza łączność z centralkami w chronionych pomieszczeniach zgodnie z ustalonymi priorytetami;
- przyjmuje sygnały alarmów;
- stanowi bazę danych o chronionych pomieszczeniach w postaci testowej i graficznej;
- kontroluje pracę strażników poprzez rejestrację czasu ich reakcji na zdarzenia;
- archiwizuje wszystkie zdarzenia zaistniałe w systemie (alarmy, awarie, zdarzenia związane z obsługą - np. zmianę danych abonenta);
- w połączeniu z odpowiednim sprzętem może automatycznie przekazywać sygnały alarmu i awarii do stacji monitorującej jeżeli agencja ochrony jest w nią wyposażona,
- umożliwia zdalne sterowanie funkcjami centralek;
- wykonuje pewne funkcje pomocnicze (kalkulator, kalendarz prosty edytor tekstów).

To tylko najważniejsze funkcje realizowane z komputera z centrum nadzoru. Rozwiązania firmowe, sposób oprogramowania komputera, czy możliwości centralek pozwalają na realizację innych funkcji. Ze względu na ograniczone ramy opracowania zostały przedstawione funkcje najważniejsze i charakterystyczne dla współczesnych systemów alarmowych.

BIBLIOGRAFIA

1) Ustawa z 23 listopada 1990 r. o łączności (Dz.U. nr 86, z póź. zm.);
2) Rozporządzenie Ministra Spraw Wewnętrznych 28 marca 1994 r. w sprawie wprowadzenia obowiązku stosowania Polskich Norm i norm branżowych (Dz.U. nr 44, poz. 174) polska norma PN-93/E-08390 Systemy alarmowe;
3) Zarządzenie nr 20 prezesa Polskiego Komitetu Normalizacji Miar i Jakości z 15 kwietnia 1986 r. w sprawie ustalenia wykazu mechanicznych i elektronicznych urządzeń zabezpieczających podlegających badaniom, ocenie i kwalifikacji;
4) Ustawa z 3 kwietnia 1993 r. o badaniach i certyfikacji (Dz.U. nr 55, poz. 250);
5) Ustawa z 23 listopada 1990 r. o łączności (Dz.U. nr 86, poz. 504);
6) Ustawa z 20 maja 1971 r. kodeks wykroczeń (Dz.U. nr 12, poz. 114);
7) Ustawa z 3 kwietnia 1993 r. o normalizacji (Dz.U. nr 55, poz. 251)
8) A. Wójcik, „Wprowadzenie do projektowania systemów sygnalizacji zagrożeń", Warszawa 1997;
9) „Systemy sygnalizacji zagrożeń i nadzoru wizyjnego", EFECTA Sp. z o.o., Warszawa 1997;
10) A. Wójcik „Wybrane elementy technicznego zabezpieczania obiektów wojskowych systemami sygnalizacji zagrożeń", EFECTA Sp. z o.o., Warszawa 1997;
11) Dwumiesięczniki branży security „Systemy alarmowe", Warszawa, 1996-1998;
12) Dwumiesięcznik „Ochrona mienia 1'98", Warszawa 1998;
13) W. Hołubowicz, P. Płóciennik, A. Różański, „Systemy łączności radiowej", Poznań 1997;
14) Dokumentacja techniczna firmy EFECTA Sp. z o.o.;
15) Dokumentacja techniczna firmy SEZAM Sp. z o.o.;
16) Dokumentacja techniczna firmy ATM S.A;
17) Dokumentacja techniczna firmy MOTOROLA;
18) Dokumentacja techniczna firmy OPTO Sp. z o.o.;
19) Dokumentacja techniczna firmy DGT Sp. z o.o.;
20) Katalog firm SECUREX'98, Międzynarodowe Targi Poznańskie, Poznań 20-23.01.1998.