Mieczysław SZUSTAKOWSKI, Wiesław CIURAPIŃSKI
Instytut Optoelektroniki, Wojskowa Akademia Techniczna, Warszawa

TECHNICZNE SYSTEMY ZABEZPIECZENIA MIENIA I INFRASTRUKTURY KRYTYCZNEJ

Abstract

Devices and security object protection systems are developing dynamically. Using them is including large areas of the social life. Improvement in the living conditions and wealth's is flowing into to the height of threatening of possessions as well as privates and public objects.

The global situation is generating terrorist attacks directed at public objects (critical infrastructure). And so building new technical security systems of such a kind of objects is needed.

The market of securities is offering many specialist systems. Using them is depending on the full service of the professionalization of the security guards. The aim of this article is showing the outline of existing technical security systems.

Streszczenie

Urządzenia i systemy technicznego zabezpieczenia mienia obiektów stanowią dzisiaj dynamicznie rozwijający się dział techniki, zastosowanie, którego obejmuje wciąż rozszerzające się obszary życia społecznego.

Wraz z poprawą warunków życia i zamożności społeczeństwa obserwuje się wzrost zagrożenia mienia i obiektów zarówno własności prywatnej jak i firm.

Sytuacja stosunków międzyludzkich w skali globalnej generuje zagrożenia aktami terrorystycznymi wymierzonymi w obiekty i instytucje użyteczności publicznej tzw. infrastruktura krytyczna.

Budowa wielkich obiektów handlowych (hipermarkety), biurowych – budynki inteligentne i użyteczności publicznej stwarzają zagrożenie życia przez ewentualne pożary lub skażenia środowiska (powietrza, wody).

Musimy, zatem budować systemy zabezpieczeń mienia i małych obiektów, głównie zagrożonych kradzieżą i wandalizmem, zabezpieczenia infrastruktury krytycznej – obiektów szczególnego znaczenia dla funkcjonowania społeczeństwa i państwa przed zagrożeniem terrorystycznym, zabezpieczenia życia w obiektach rozległych mieszczących jednocześnie duże zbiorowiska ludzi zagrożonych głównie pożarem lub skażeniem środowiska.

Rynek systemów zabezpieczeń oferuje specjalizowane systemy ochrony mienia, infrastruktury krytycznej, życia, których skuteczność w dużej mierze zależy od umiejętności ich stosowania i włączenia w system bezpieczeństwa wspomagany interwencją ochrony fizycznej i procedurami postępowania.

Celem niniejszej pracy jest przedstawienie zarysu istniejących systemów zabezpieczeń technicznych szczególnym uwzględnieniem systemów ochrony mienia i obiektów. Systemy ochrony infrastruktury krytycznej i zabezpieczenia życia zostaną tylko zasygnalizowane.

1. UWARUNKOWANIA PRAWNE STOSOWANIA TECHNICZNYCH SYSTEMÓW OCHRONY MIENIA I INFRASTRUKTURY KRYTYCZNEJ

Stosowanie technicznych systemów ochrony mienia oraz warunki funkcjonowania branży zawodowej tzn. firm i osób związanych z stosowaniem systemów ochrony technicznej określa „Ustawa o ochronie osób i mienia" z dnia 22 sierpnia 1997r., wraz z rozporządzeniami wykonawczymi.

Ustawa (art.1) określa:

1. Obiekty i urządzenia podlegające obowiązkowej ochronie.
2. Zasady tworzenia i funkcjonowania wewnętrznych służb ochrony.
3. Zasady prowadzenia działalności gospodarczej w zakresie usług ochrony osób i mienia.
4. Wymagania, kwalifikacje i uprawnienia pracowników ochrony.

5. Ustanawia nadzór nad funkcjonowaniem ochrony osób i mienia.

Artykuł 3 ustawy określa realizację ochrony osób i mienia w formie:

1. Bezpośredniej ochrony fizycznej.
2. Zabezpieczenia technicznego polegającego na:
   a) montażu elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia oraz eksploatacji, konserwacji i naprawach w miejscach ich zainstalowania,
   b) montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach ich zainstalowania.

Ustawa określa obszary, obiekty i urządzenia ważne dla obronności, interesu gospodarczego państwa i bezpieczeństwa publicznego, które podlegają obowiązkowej ochronie przez uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne.

Szczegółowe wykazy obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie sporządzają ministrowie lub kierownicy urzędów centralnych. Ewidencję bieżącą prowadzą wojewodowie. Każdy kierownik obiektu podlegającego szczegółowej ochronie sporządza plan ochrony, który uzgadnia z odpowiednim terytorialnie komendantem policji.

W ten sposób ustawa określiła pole działania osób i firm ochrony technicznej i fizycznej. W odniesieniu do osób i firm realizujących ochronę techniczna ustawa określa wymagania posiadania odpowiednio licencji (osoby) i koncesji (firmy) wydawanych przez wojewódzkie komendy policji.

Wymienione w „Ustawie o ochronie osób i mienia" z 1997r. „Obszary, obiekty i urządzenia podlegające obowiązkowej ochronie zostały w Ustawie z dnia 26.04. 2007r, dotyczącej zarządzania kryzysowego, określone jako „infrastruktura krytyczna". Zgodnie z treścią tej ustawy przez określenie infrastruktura krytyczna – należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię i paliwa;
b) łączności i sieci teleinformatycznych;
c) finansowe;
d) zaopatrzenia w żywność i wodę;
e) ochrony zdrowia;
f) transportowe i komunikacyjne;
g) ratownicze;
h) zapewniające ciągłość działania administracji publicznej;
i) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochrona infrastruktury krytycznej – to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej na wypadek zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.

Analizując łącznie treść obu ustaw (tzn. „O ochronie osób i mienia" z dnia 22.08.1997r. i „Zarządzaniu kryzysowym" z dnia 26.04.2007r.) można zdefiniować rolę i zadania systemów ochrony technicznej:

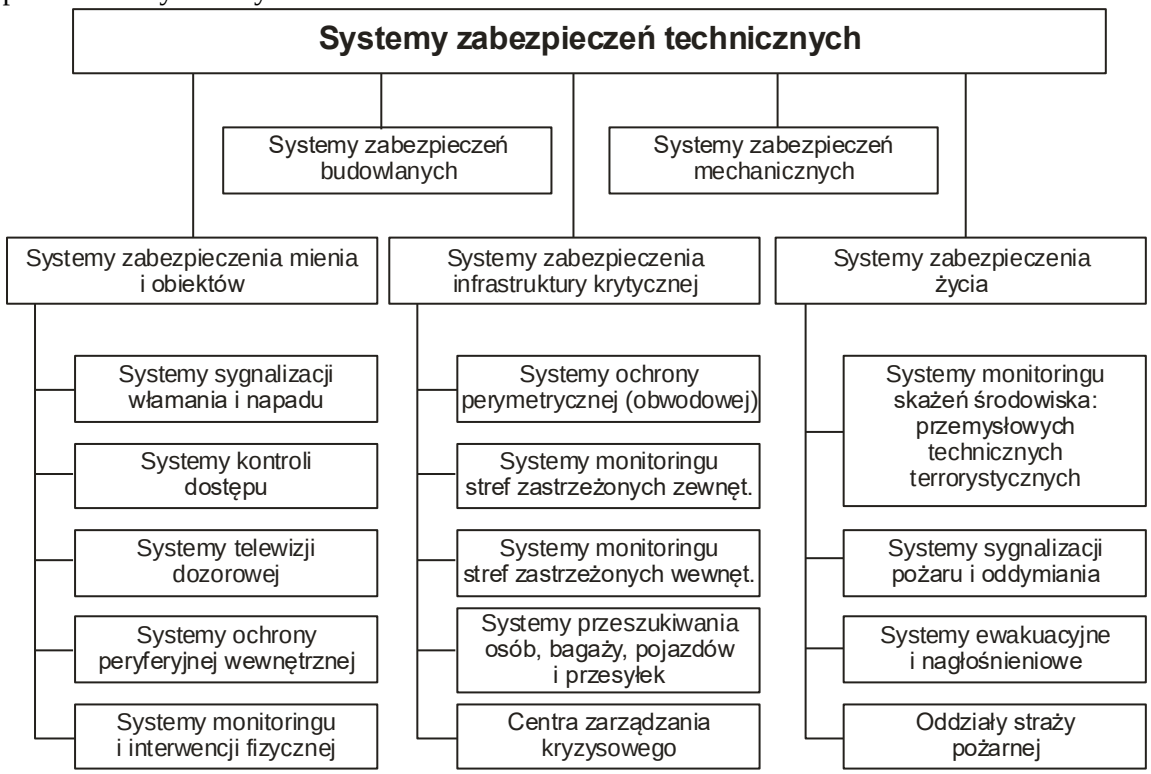
a) zabezpieczenie (ochrona) mienia, obiektów, osób prywatnych, firm i przedsiębiorstw głównie przed kradzieżą i dewastacją;
b) zabezpieczenie (ochrona) przed spowodowaniem sytuacji kryzysowych w obiektach i systemach określanych infrastrukturą krytyczną. Sytuacją kryzysową w rozumieniu Ustawy z 2007r. to sytuacja będąca następstwem zagrożenia lub działania przestępczego (terrorystycznego) przy jednoczesnym zakłóceniu funkcjonowania obiektu, przedsiębiorstwa, instytucji.

Zatem w odniesieniu do infrastruktury krytycznej celem stosowania systemów zabezpieczeń to przeciwdziałanie spowodowania zagrożenia lub zakłócenia funkcjonowania obiektu.

We wszystkich wymienionych zwłaszcza dużych obiektach stosuje się systemy zabezpieczenia życia. Są to głównie systemy przeciw pożarowe, ewakuacyjne, nagłośnieniowe.

Do systemów zabezpieczenia życia zalicza się również systemy monitoringu zagrożeń przemysłowego oraz technicznego i terrorystycznego skażenia środowiska (powietrza, wody). W

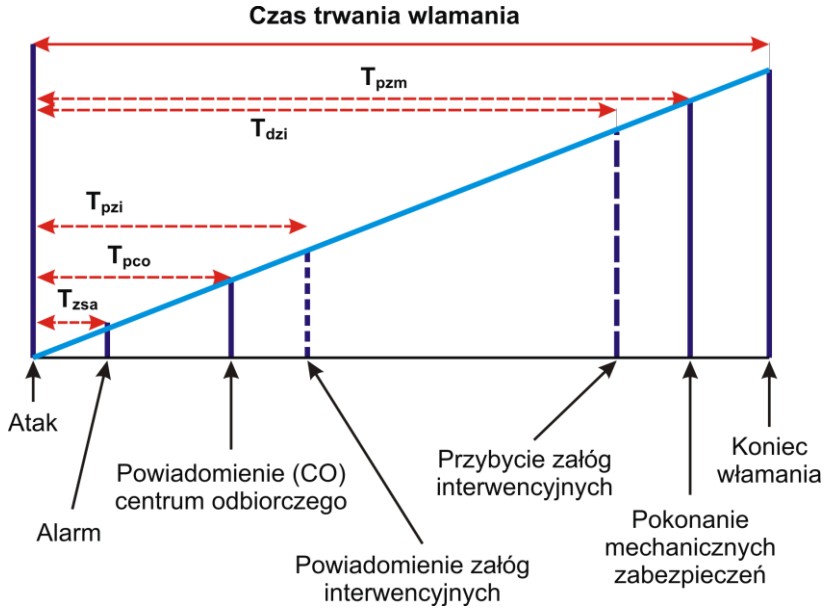
świetle przywołanych wyżej ustaw możemy wyróżnić trzy działy elektronicznych, odpowiednio wyspecjalizowanych systemów zabezpieczeń, oraz dział zabezpieczeń budowlanych i mechanicznych przedstawionych na rys.1.



Rys.1. Systemy zabezpieczenia technicznego.

Systemy zabezpieczeń budowlanych i mechanicznych są stosowane powszechnie we wszystkich trzech wyróżnionych rodzajach zabezpieczeń objętych systemami zabezpieczeń elektronicznych.

Zabezpieczenia budowlane i mechaniczne oraz zabezpieczenia elektroniczne i czas interwencji fizycznej powinny być wzajemnie skorelowane w sposób umożliwiający skuteczne przeciwdziałanie kradzieży lub dewastacji mienia (rys. 2).



Rys. 2. Zasada skutecznej interwencji.

Systemy ochrony mienia, obiektów, osób prywatnych i firm są monitorowane przez wyspecjalizowane firmy monitorowania alarmów i interwencji fizycznej w przeciągu ustalonego przedziału czasu (5-10 minut).

Systemy zabezpieczenia infrastruktury krytycznej są z reguły nadzorowane przez Centra Nadzoru z całodobowym dyżurem operatorskim i zarządzane przez Centra Zarządzania Kryzysowego lokalne w danym obiekcie infrastruktury (np. lotniska, rafinerie) lub terytorialne (gminne, powiatowe, wojewódzkie).

Systemy zabezpieczenia życia w obiektach publicznych są nadzorowane przez lokalne i terytorialne jednostki straży pożarnej. Straż pożarna jest również jednostką interweniującą we wszystkich przypadkach pożaru bez względu na rodzaj obiektu.

2. ZASADY BUDOWY, SPOSÓB STOSOWANIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ, UPRAWNIENIA ZAWODOWE

Zasady budowy, dobór urządzeń i warunki eksploatacji elektronicznych systemów zabezpieczeń mienia, obiektów i infrastruktury krytycznej określają:

1. Normy Polskie dotyczące poszczególnych systemów.
2. Wymagania ubezpieczycieli dotyczące obiektów i mienia ubezpieczanego.
3. Zarządzenia resortowe dotyczące obiektów szczególnego znaczenia – infrastruktury krytycznej.

2.1. Polskie Normy

Normy Polskie dotyczące systemów zabezpieczeń są z reguły tłumaczeniem norm europejskich i są wydawane w seriach dotyczących poszczególnych systemów. Normy określają dobór urządzeń i zabezpieczeń mechanicznych: drzwi, okien, krat, sejfów oraz elektronicznych systemów w stosunku do wartości chronionego mienia. Normy określają również warunki budowy systemu, doboru urządzeń, zasilania, komunikacji wewnątrz systemowej, zapisu i przechowywania informacji, monitorowania łączności i powiadamiania właściciela.
Zestaw norm można znaleźć w Internecie pod adresem:
http://www.alarmy.m3m.pl/polskie_normy_dla_alarmow.html

2.2. Wymagania ubezpieczycieli

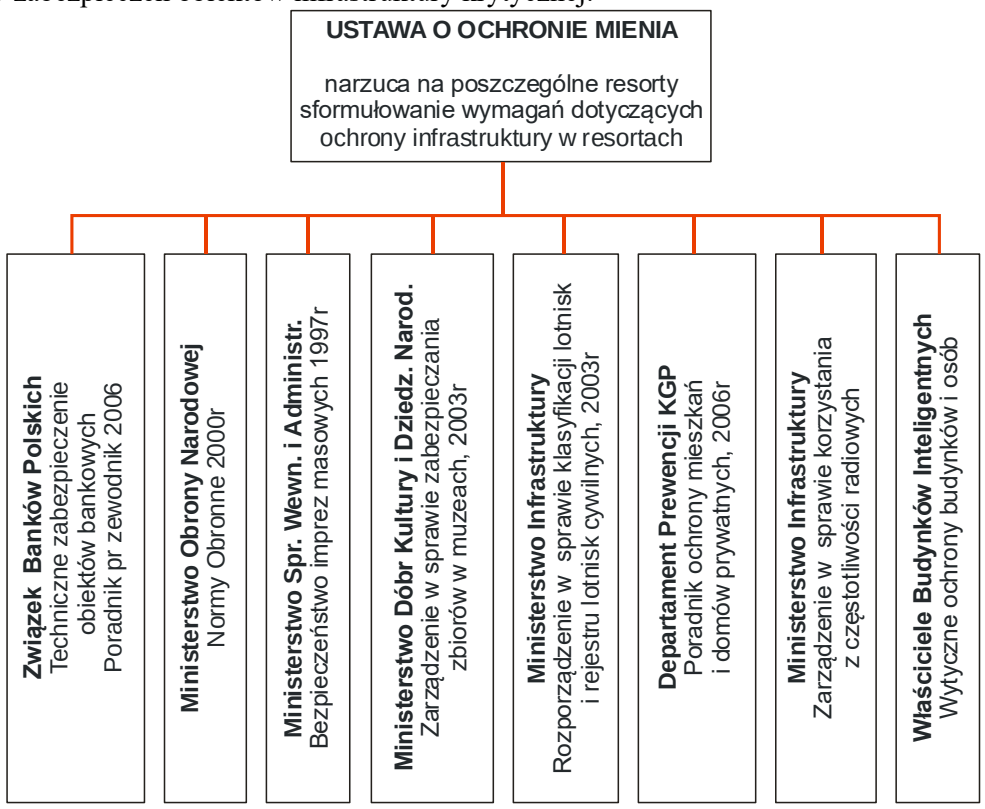
Istotną rolę w kształtowaniu budowy systemu zabezpieczeń maja wymagania ubezpieczycieli. Firma instalująca system ochrony dowolnego obiektu powinna uwzględnić wymagania właściwego ubezpieczyciela. W Polsce na razie nie ma porozumienia ogólnokrajowego ubezpieczycieli odnośnie wymagań systemu zabezpieczeń. Należy zatem uwzględniać indywidualne wymagania ubezpieczycieli, albowiem koszty ubezpieczenia są skorelowane z systemem zabezpieczeń. Dla przykładu: Firma ubezpieczeniowa Warta w polisie Dom Komfort oferuje następujące zniżki rocznych opłat:

1. system alarmowy z monitoringiem i interwencją fizyczną – 30%;
2. całodobowy dozór lokalny – 30%;
3. drzwi przeciwwłamaniowe z certyfikatem – 20%;
4. bezszkodowy przebieg ubezpieczenia do 20%;
5. kraty, rolety przeciwłamaniowe w oknach – 10%;
6. system alarmowy – 10%;
7. zamek z certyfikatem – 5%;
8. blokady antywłamaniowe – 5%.

2.3. Zarządzenia resortowe

Systemy zabezpieczenia obiektów infrastruktury krytycznej są budowane wg wymagań sformułowanych przez poszczególne resorty. Ustawa o ochronie mienia z 22.08.1997r. zobowiązuje poszczególne resorty do opracowania planów ochrony obiektów szczególnie ważnych dla funkcjonowania państwa. Ustawa z 26.04.2007r. definiuje podobne obiekty jako infrastrukturę krytyczną. Można, zatem używając współcześnie obowiązującego słownictwa wytyczne resortowe

ochrony obiektów szczególnego znaczenia traktować jako wytyczne ochrony obiektów infrastruktury krytycznej. W tabeli 1 podano zestaw aktualnych zarządzeń resortowych dotyczących elektronicznych systemów zabezpieczeń obiektów infrastruktury krytycznej.



Tab.1. Wytyczne resortowe elektronicznych systemów zabezpieczeń obiektów infrastruktury krytycznej.

2.4. Uprawnienia zawodowe

Uprawnienia zawodowe upoważniające do instalacji i projektowania systemów ochrony uzyskuje się na podstawie licencji wydawanych przez wojewódzkie Komendy Policji. Kursy zawodowe uprawniające do uzyskania licencji pracownika technicznego systemów ochrony, prowadzą Zrzeszenia firm branży technicznego zabezpieczenia mienia. Są to Polska Izba Ochrony Osób i Mienia, Polska Izba Systemów Alarmowych, Ogólnopolskie Stowarzyszenie Inżynierów i Techników Systemów Zabezpieczeń. Ww. Zrzeszenia prowadzą:

1. Kursy instalatorów – licencja I stopnia;
2. Kursy projektantów – (licencja II stopnia);
3. Kursy ekspertów (biegły sądowy).

Powyższe licencje I i II stopnia można również otrzymać po ukończeniu studiów politechnicznych, inżynierskich, magisterskich lub podyplomowych z specjalności inżynieria systemów ochrony np. w Wojskowej Akademii Technicznej.

3. URZĄDZENIA ORAZ ZABEZPIECZENIA BUDOWLANE I MECHANICZNE

Użycie mechanicznych zabezpieczeń jest najstarszym sposobem ochrony mienia, obiektów i obszarów. Można by rzec że od czasów prehistorycznych do dzisiejszych człowiek rozwijał i rozwija mechaniczne zabezpieczenia swojej własności w odniesieniu do mienia, domu, obszaru. Dzisiaj zabezpieczenia budowlane i mechaniczne odnosimy do wytrzymałości ścian, stropów, pomieszczeń, zabezpieczenia otworów, okien, drzwi i urządzeń przechowywania wartości: szaf, sejfów, skarbców, pomieszczeń – kancelarii tajnych jako przechowywania dokumentów, informacji, jak również

magazynów i składów, obszarów, portów lotniczych i morskich, jednostek wojskowych, przedsiębiorstw itp.

Projektant systemu zabezpieczeń dysponuje dzisiaj katalogiem znormalizowanych urządzeń zabezpieczenia mechanicznego ujętych w kategorie pod względem wytrzymałości mechanicznej (szyby, drzwi, ściany, stropy, kraty) pod względem czasu otwarcia lub wyłamania – zamki, sejfy, szafy, mechaniczne bariery utrudniające dostęp - kołowroty, szlabany, bariery itp., które ułatwiają współpracę z elektroniczną kontrolą dostępu.

Potwierdzenie cech charakterystycznych dla danej kategorii urządzenia projektant uzyskuje analizując świadectwo – certyfikat – jakości danego urządzenia.

Jakie kategorie wytrzymałości urządzeń mają być zastosowane, w jakich sytuacjach i do chronienia jakich wartości określają normy techniczne i zarządzenia (przepisy) resortowe.
Np. norma techniczna określająca kategorie wytrzymałościowe urządzeń i ich powiązanie z klasyfikacją zagrożeń mienia, obiektów, obszarów PNEN-1143-1:2000.

4. ELEKTRONICZNE URZĄDZENIA I SYSTEMY ZABEZPIECZENIA MIENIA I OBIEKTÓW

Terminologia ustawowa „techniczne zabezpieczenia" została w gwarze środowiskowej zastąpiona określeniem „systemy ochrony" (domyślnie elektroniczne). W tabeli na rys. 1 przedstawiono elektroniczne systemy używane dla ochrony mienia i obiektów. Nazwy poszczególnych systemów sugerują przeznaczenie systemów. Do ochrony mienia i obiektów najczęściej są używane zintegrowane systemy złożone z niżej wymienionych systemów:
- sygnalizacje włamania i napadu (SWiN),
- system kontroli dostępu (SKD),
- telewizji dozorowej (CCTV –ang. Close Circuit Television),
- systemy ochrony zewnętrznej obiektu(SOZ).

Każdy z wyżej wymienionych systemów obejmuje co najmniej 3 rodzaje systemów określające ich zastosowanie w małych, średnich i dużych obiektach, różniące się strukturą i organizacją wewnętrzną.

Ponadto systemy SWiN, SKD, CCTV i SOZ posiadają sobie właściwe urządzenia pozyskujące informacje zwane czujkami, czytnikami, kamerami, barierami, kablami czujnikowymi. W niniejszym opracowaniu brak jest miejsca na pełną prezentacje systemów i ich oprzyrządowanie. Celem naszym jest pokazanie rozległej różnorodności technicznej jaką dysponuje projektant elektronicznych systemów ochrony mienia. Dlatego wymienimy tylko jako ilustrację podstawowe rodzaje systemów.

4.1. System Sygnalizacji Włamania i Napadu.

Jest to podstawowy system sygnalizujący włamanie do danego obiektu. Bazową jednostką systemu SWiN jest Centrala Alarmowa która zbiera i przetwarza informacje pozyskaną z dołączonych o niej czujek. Czujkami są urządzenia sygnalizujące zmiany otoczenia wnoszone przez intruza.

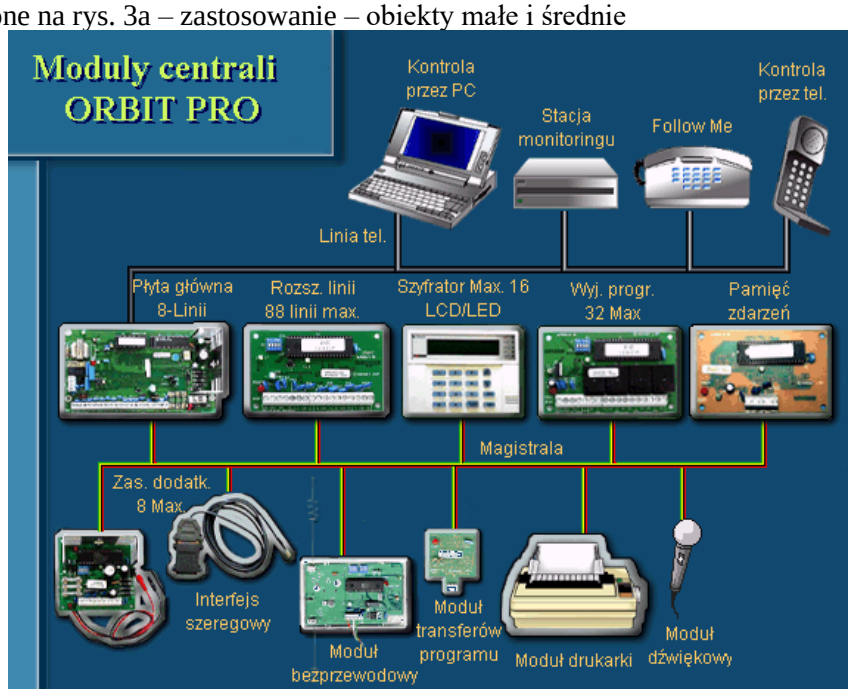
Czujki PIR –wykrywają temperaturę intruza różną od otoczenia, czujki zbicia szyb – rejestrują dźwięki tłuczenia szyby. Czujki wyłamania drzwi, przebicia ściany – rejestrują drgania wytwarzane przy tej czynności itd. Czujki same przetwarzają sygnały i same decydują a raczej wypracowują stan alarmu o czym powiadamiają Centralę, która z kolei przekazuje sygnał alarmu operatorowi w zaprogramowany sposób.

Czujki powiadamiają również centralę np. o zasłonięciu czujki - sabotaż, o przerwaniu zasilania. Centrala zaś kontroluje stan łączności. A zatem system już ten najprostszy jak pokazany na rys. 3a jest złożona konstrukcja techniczna, bazująca na sieci teleinformatycznej z odpowiednim okablowaniem, oprogramowaniem i oprzyrządowaniem o znamionach automatycznego działania.

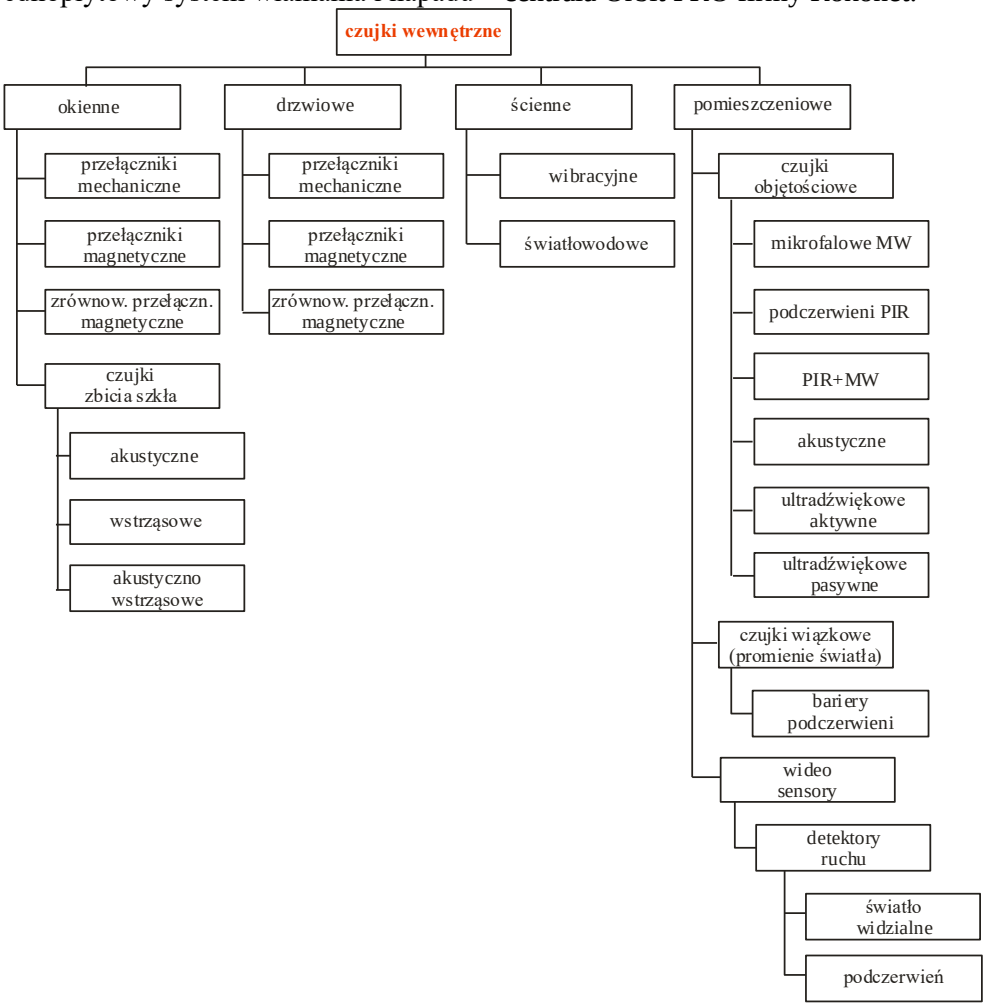
Systemy włamania i napadu w sensie central, struktury organizacyjnej, urządzeń (kontrolery sieciowe, ekspandery itp.) i oprogramowania są wytwarzane przez wyspecjalizowane firmy jako systemy firmowe, zamknięte. System komunikacji wewnętrznej, oprogramowanie, technologia urządzeń są chronione przez poszczególne firmy. Natomiast czujki (rys. 3b) aczkolwiek też wytwarzane przez firmy są urządzeniami które mogą być stosowane w wielu systemach gdyż

posiadają określony standardem sposób komunikowania się z centralą. W zbiorze systemów sygnalizacji włamania i napadu wyróżniamy:

1. Systemy bazujące na Centralach Alarmowych jednopłytowych w skrócie systemy jednopłytowe przedstawione na rys. 3a – zastosowanie – obiekty małe i średnie

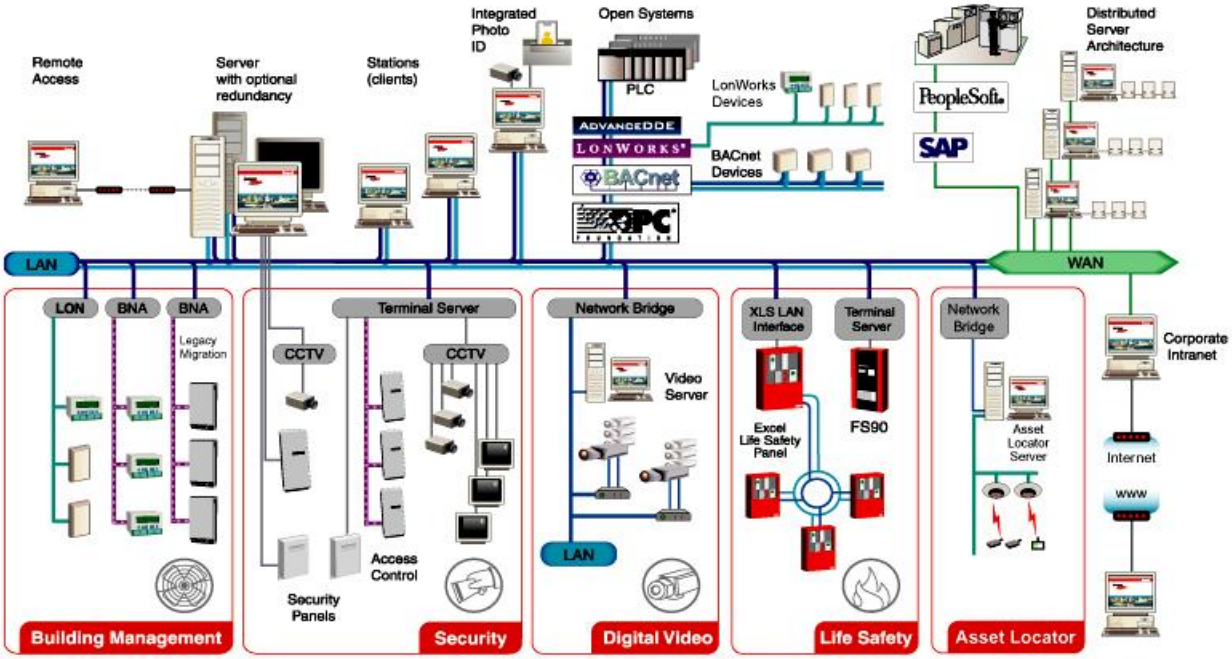


Rys. 3a. Jednopłytowy system włamania i napadu – centrala Orbit PRO firmy Rokonet.



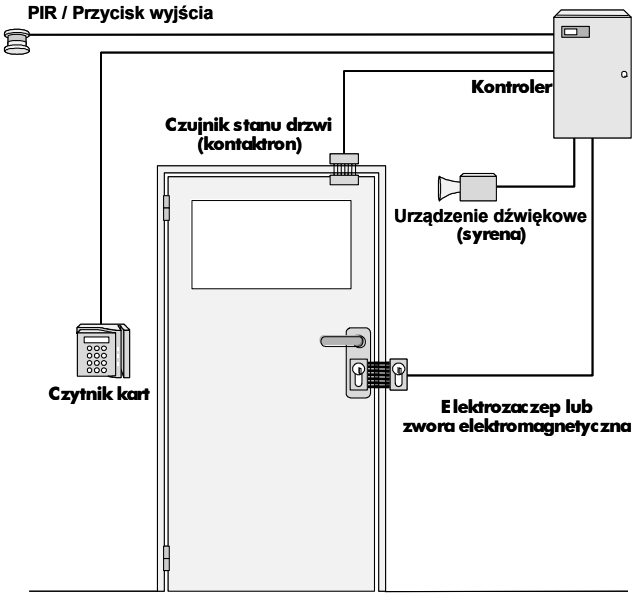
Rys. 3b. Czujki systemu włamania i napadu.

2. Systemy komputerowe w których jako Centrale Alarmowe stosuje się komputer z odpowiednim oprzyrządowaniem. Systemem steruje tzw. kontroler (lub kontrolery) sieciowy i odpowiednie urządzenia stanowiące interfejsy systemu do podłączania czujek jako produktów innych firm.
3. Systemy bazujące na Integratorze Systemów. Przykładem takiego systemu jest system firmy Honeywell (rys. 4). Podobne wyspecjalizowane systemy posiadają wielkie światowe firmy jak Simens, Bosch, Magal czy Thales. System integruje w ramach sieci np. Ethernet wiele różnorodnych systemów często różnych producentów. Integratorem systemu jest komputer zwany tutaj serwerem a istotą systemu jest oprogramowanie zarządzające całością systemu oraz interfejsy programowe tłumaczące „języki" programowe poszczególnych systemów na język programowy Integratora.



Rys. 4. Zintegrowany system ochrony Budynku Inteligentnego firmy Honeywell, integrujący ochronę, automatykę i zarządzanie budynkiem.

4.2. System kontroli dostępu



Rys.5. Schemat oprzyrządowania kontroli dostępu

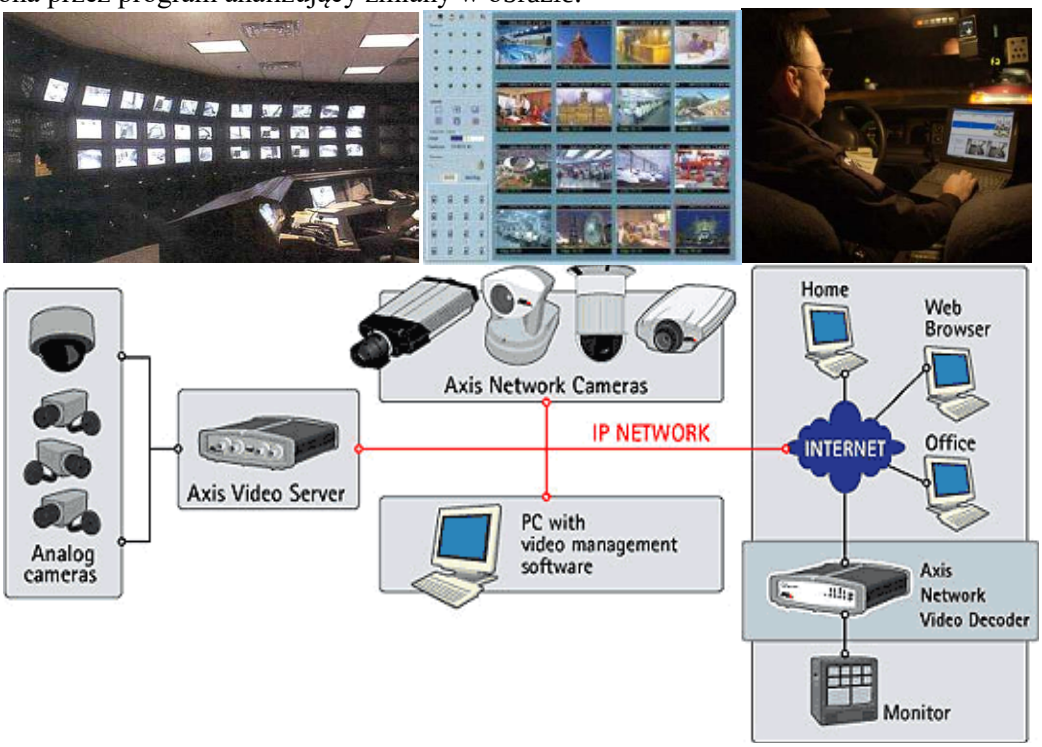
Umożliwia elektroniczną kontrolę osób wchodzących (wychodzących) do danego obiektu. Kontrola tożsamości osób odbywa się na podstawie:
- karty elektronicznej z kodem danej osoby,
- podanego kodu numerycznego (PIN),
- cech biometrycznych.

Identyfikacji osoby można dokonać porównując wcześniej zdjęte i zarejestrowane cechy biometryczne z cechami osoby odczytanymi przez czujnik biometryczny na wejściu. Dokładność czy skuteczność kontroli osób zależy więc od rodzaju zastosowanych czytników bądź ich kombinacji. Schemat działania i oprzyrządowania wejścia przy elektronicznej kontroli osób ilustruje rys. 5.
Systemy kontroli dostępu mogą być stosowane jako:
1. automatyczne (pojedyncze) czytniki kontrolujące jedno wejście;
2. autonomiczne kontrolery – kontrolujące kilka wejść;
3. system komputerowy kontrolujący poruszanie się setek osób w danym obiekcie.

4.3. Systemy dozoru wizyjnego

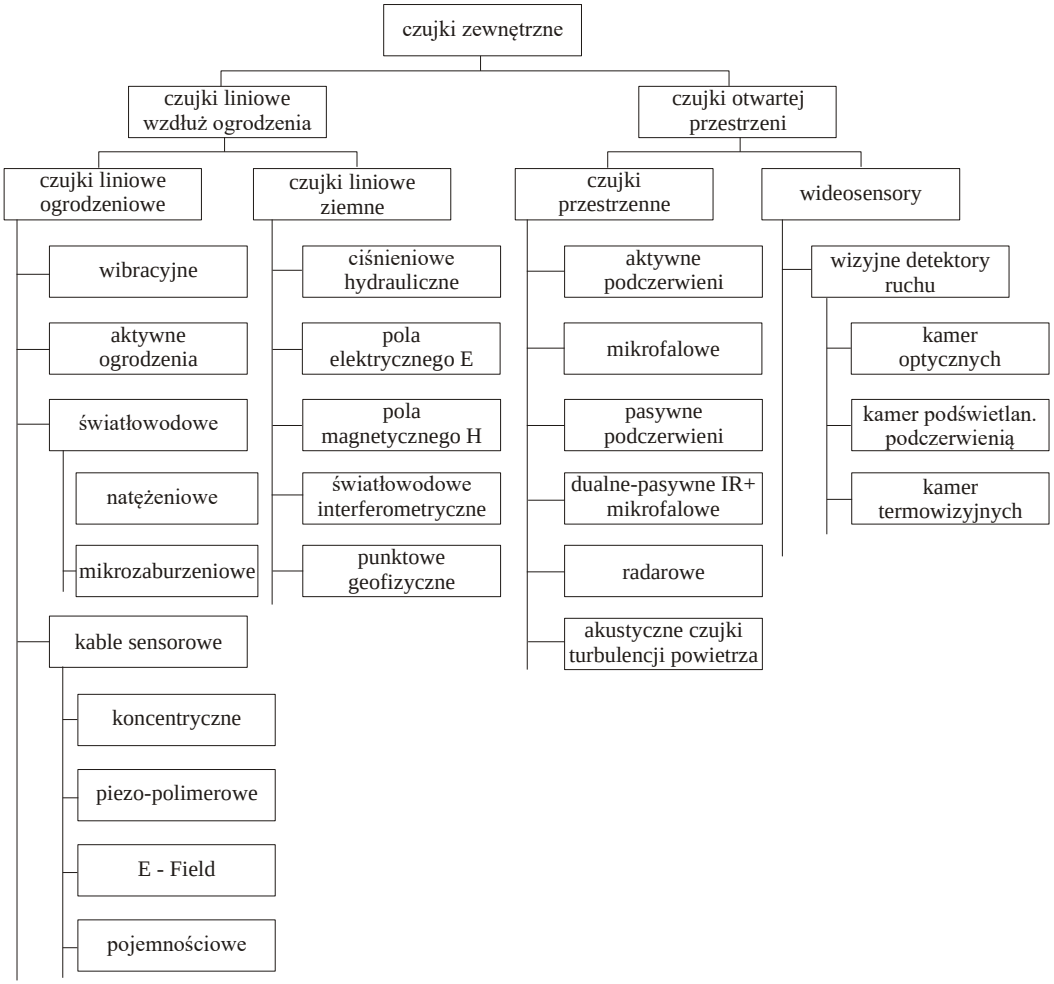
Systemy wizyjne używane w systemach ochrony należą do najbardziej dynamicznie rozwijających się technologii branży ochrony technicznej obiektów. Aktualnie rozróżniamy:
1. systemy telewizji dozorowej – tzw. systemy obserwacyjne (analogowe),
2. systemy telewizji dozorowej – detekcyjne (detekujące ruch w polu widzenia kamery),
3. systemy telewizji dozorowej – inteligentne (analizujące zmiany scenerii w polach oznaczonych w polu widzenia kamery),
4. systemy telewizji dozorowej – sieciowe (systemy cyfrowe budowane na bazie teleinformatycznej sieci Ethernet – IP).

Na rys. 6 przedstawiono mieszany system telewizyjny z oprzyrządowaniem firmy AXIS jaki aktualnie najczęściej powstaje przy modernizacji wcześniejszych systemów analogowych przez współczesne cyfrowe systemy sieciowe.
Na rys. 6 u góry przedstawiono Centrum Nadzoru telewizji dozorowej obserwacyjnej gdzie człowiek był zmuszony analizować obraz każdej kamery w każdym momencie. Stąd powstawała ściana monitorów i kilka wpatrzonych w nie operatorów. Z prawej strony u góry jedno ekranowa stacja obserwacji kamerowej telewizji cyfrowej. Tutaj każda kamera rejestruje swój obraz a do Centrum przekazuje tylko obraz z sytuacji alarmowej. Zatem obserwacja obrazu przez człowieka została zastąpiona przez program analizujący zmiany w obrazie.



Rys. 6. Schemat funkcjonalny telewizji cyfrowej sieciowej.

4.4. Systemy ochrony zewnętrznej



Rys. 7. Czujniki systemu ochrony zewnętrznej

Systemy ochrony zewnętrznej obiektu to oddzielny rozbudowany dział systemów liniowych służących do ochrony obwodowej zarówno małych posesji i obiektów, jak i infrastruktury krytycznej (lotnisk, fabryk, granic). W tabeli na rys. 7 podano stosowane urządzenia czujnikowe. Są to liniowe czujniki kablowe mocowane na ogrodzeniach lub zakopywane w gruncie albo nawierzchniowe bariery mikrofalowe lub podczerwieni. Systemy czujników lokalizowanych w obwodnicy danego obszaru są wspomagane przez systemy telewizji CCTV, systemy termo wizji i radary naziemne. Całość funkcjonuje jako zintegrowany system ochrony obwodowej obszaru z Centrum Nadzoru.

5. INTEGRACJA SYSTEMÓW OCHRONY MIENIA I OBIEKTÓW

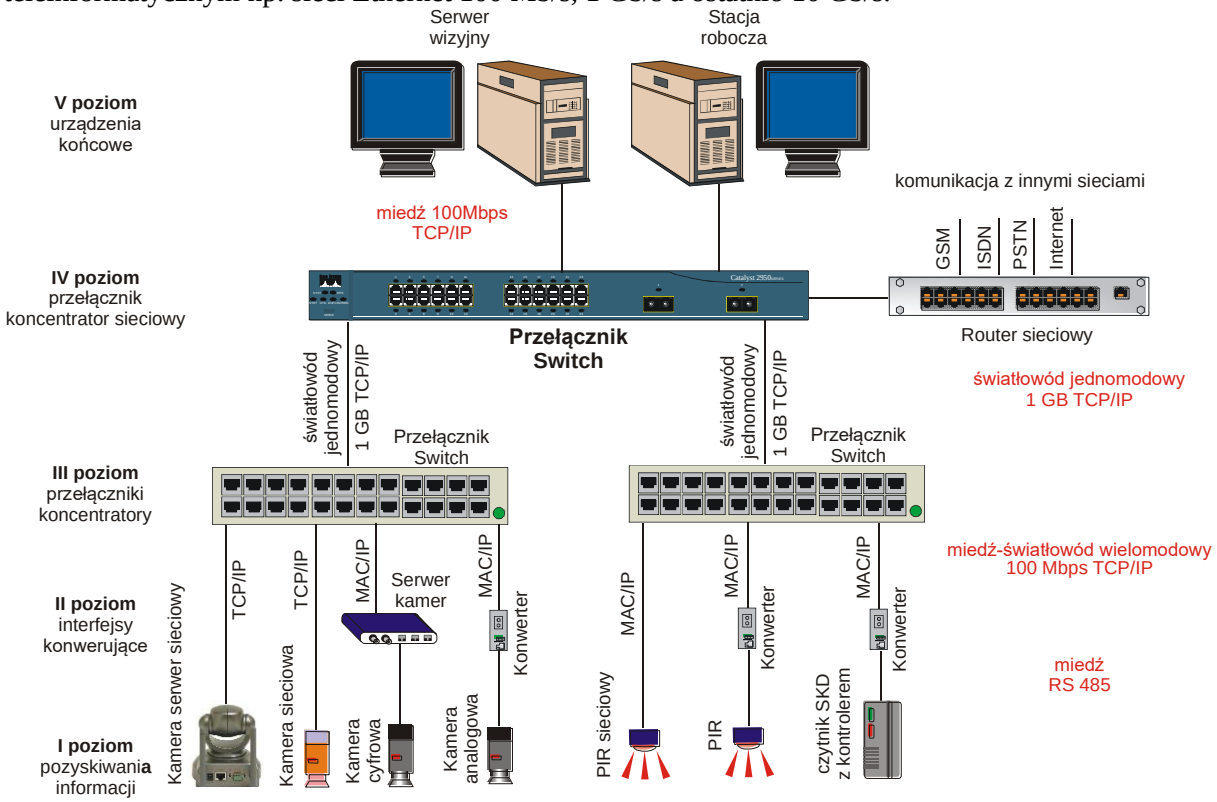
Rzadko nawet w małych obiektach stosuje się jednorodne elektroniczne systemy ochrony. Najczęściej są to systemy złożone z elementów kilku systemów noszące nazwę systemów zintegrowanych. Integracja systemów może się odbywać na bazie strukturalnej każdego z wyżej przedstawionych systemów. Rozróżniamy zatem systemy:

- integrowane na bazie SWiN;
- integrowane na bazie SKD;
- integrowane na bazie CCTV;
- integrowane na bazie Integratora Systemów.

W tym ostatnim przypadku mamy już System Systemów – dotyczy to Integratorów stosowanych w dużych systemach jak np. Budynki Inteligentne.

Technologia elektronicznych systemów ochrony jest w ciągłym rozwoju, zarówno pod względem konstrukcji jak i przetwarzania sygnałów. Aktualnie w powszechnym użyciu są cyfrowe systemy przetwarzania sygnału (DSP – Digital Signal Processing) np. czujki PIR czy mikrofalowe

wykrywające oddzielnie zmiany termiczne i ruch w polu widzenia znane są jako czujki wielo detektorowe w jednej obudowie. Jako rekordową można przytoczyć czujkę firmy Bosch pięcio detektorową: PIR – bliski (3-4 m), PIR – daleki (15-18m), mikrofala (15-18 m), detektor światła białego i detektor temperatury.
Procesor wypracowuje alarm według określonego algorytmu na podstawie danych 5 detektorów odnoszących się do tej samej sytuacji. Znamienna jest również ewolucja protokołów komunikacji wewnątrz systemowej. Firmy produkujące wielkie systemy operujące według firmowych protokołów tworzą systemy zamknięte operujące z sobie właściwym oprzyrządowaniem i oprogramowaniem. Konkurencją dla systemów zamkniętych są systemy otwarte bazujące na sieciowym oprzyrządowaniu teleinformatycznym np. sieci Ethernet 100 Mb/s, 1 Gb/s a ostatnio 10 Gb/s.



Rys. 8. Sieciowy system otwarty.

Na rys. 8 przedstawiono sieciowy system otwarty. Do uruchomienia systemu potrzebne jest oprogramowanie aplikacyjne komputerów w Centrum Nadzoru i na poziomie czujek, czytników, kamer. Łączność wewnątrz – systemu bazuje na ogólnodostępnym oprzyrządowaniu i oprogramowaniu sieci Ethernet IP.

ZAKOŃCZENIE

Rozwój technicznych systemów zabezpieczeń nadąża za wymogami bezpieczeństwa.
Dzisiaj możemy wyróżnić trzy grupy systemów zabezpieczeń wyspecjalizowanych w ochronie:
- mienia i obiektów osób prywatnych i firm;
- infrastruktury krytycznej, czyli obiektów szczególnego znaczenia dla bezpieczeństwa społecznego (zbiorowego) i państwa;
- życia szczególnie w obiektach użyteczności publicznej, dużych halach handlowych i sportowych obiektach przemysłowych itp.

Specjalizacja metod i systemów ochrony wymusza przygotowanie specjalistów i firm, co z kolei nakłada określone zobowiązania względem uczelni i stowarzyszeń organizujących studia i kursy zawodowe w zakresie inżynierii systemów ochrony.

Literatura

1. Polska Norma PN –93/E – 089830/1-14/.
2. Ogólne warunki ubezpieczenia (OWW) – określają Pr PN (130) firmy ubezpieczeniowe.
3. Norma Europejska EN –50131-1:1997r. - klasy ochrony.
4. PNEN –50136-2-3 – określa wymagania dla urządzeń stosowanych w systemach transmisji cyfrowej Central Alarmowych z wbudowanym komunikatorem cyfrowym
5. PN-EN –1143-1 i 2000 – pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja metod badań odporności na włamanie, szafy, drzwi do pomieszczeń.
6. PN-EN – 122092:2004 (U) – klasy zamków – oznaczona cyframi arabskimi 1-5 (wymagania rosnące)
7. PN-EN –356:2000 – klasyfikacja szyb ochronnych.
8. Ustawa o zamówieniach publicznych
9. Z. Nowicki *Alarm o przestępstwie*. Poradnik dla instalatorów i użytkowników systemów alarmowych oraz dla reagujących na sygnał alarmu". Wyd. Dom Organizatora, 1997.